

CA1
IST 800

-1997
E001

Government
of Canada

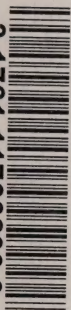
Gouvernement
du Canada

Government
Publication


The Protection of Personal Information

Building Canada's
Information Economy
and Society

3 1761 11766299 9



Canada



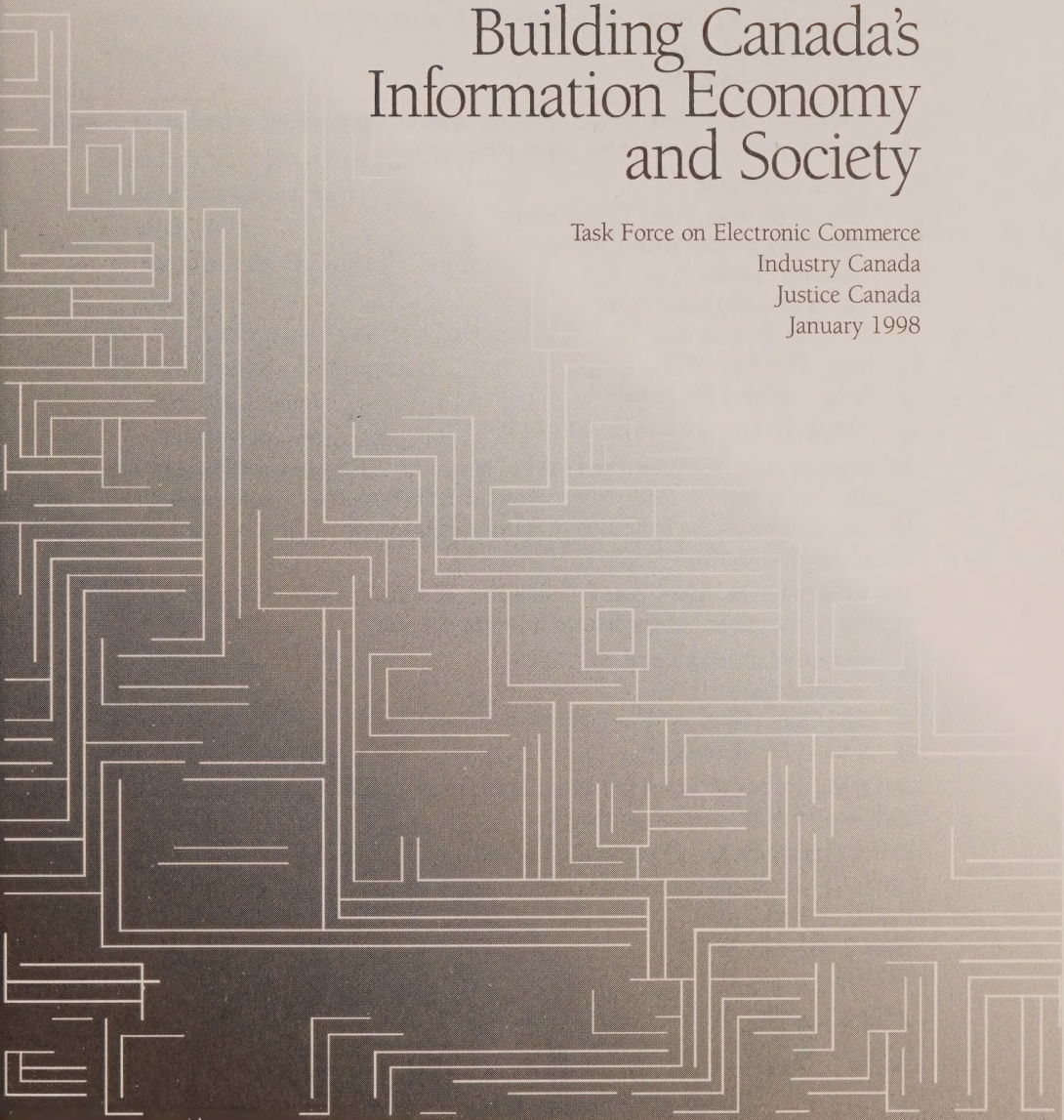
Digitized by the Internet Archive
in 2022 with funding from
University of Toronto

<https://archive.org/details/31761117662999>

The Protection of Personal Information

Building Canada's Information Economy and Society

Task Force on Electronic Commerce
Industry Canada
Justice Canada
January 1998



The Protection of Personal Information — Building Canada's Information Economy and Society is available electronically in both official languages, on the Industry Canada Strategis web site at: <http://strategis.ic.gc.ca/privacy>

It is also available on the Justice Canada web site at: <http://canada.justice.gc.ca>

This document can be made available in alternative formats for persons with disabilities upon request.

Additional print copies of this discussion paper are available from:

Distribution Services
Industry Canada
Room 205D, West Tower
235 Queen Street
Ottawa ON K1A 0H5
Tel.: (613) 947-7466
Fax: (613) 954-6436

For information about the contents of this discussion paper and the consultation process, or to submit your responses to the paper, please contact:

Helen McDonald
Director General, Policy Development
Task Force on Electronic Commerce
Industry Canada
20th Floor, 300 Slater Street
Ottawa ON K1A 0C8
Fax: (613) 957-8837
E-mail: privacy@ic.gc.ca
Telephone Enquiries: (613) 990-4255

Submissions must be received on or before March 27, 1998 and must cite the *Canada Gazette*, Part 1, Jan. 24, 1998, Notice Number IPPB-002-98 — Release of Public Discussion Paper on the Protection of Personal Information in the Marketplace and the title of this document.

Two weeks after the closing date for comments, all submissions will be made available for viewing by the public, during normal business hours at:

Industry Canada Library
3rd Floor West
235 Queen Street
Ottawa ON K1A 0H5

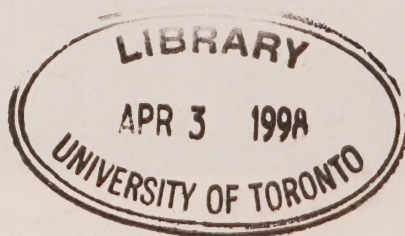
and at the regional offices of Industry Canada in Halifax, Montreal, Toronto, Edmonton and Vancouver for a period of one year.

© Her Majesty the Queen in Right of Canada
(Industry Canada/Justice Canada) 1998

Cat. No. C2-336/1998

ISBN 0-662-633-26-1

51730B



AZN-2381

Contents

Introduction: Building Canada's Information Economy and Society	1
Connecting Canadians	1
Protecting Personal Information	2
<hr/>	
Part 1: What Is Privacy?	5
What Protection Exists Now?	5
Why Current Protection is No Longer Enough	6
Protecting Personal Information: The Rules of the Road	8
The CSA Standard	9
<hr/>	
Part 2: Designing Canada's New Privacy Law	11
Ensuring Protection across Canada	11
Finding Basic Principles	12
Sectoral Codes	15
Recognition of Sectoral Codes	16
Approval	17
Ensuring Compliance with the Law and Effective Redress of Complaints	18
Accountability	18
Response to Complaints	20
Oversight Agencies	20
Public Education	21
Striking the Right Balance for Made-in-Canada Legislation	22
<hr/>	
Part 3: Your Turn	25
Obligations	25
Powers	26
Distribution of Powers and Responsibilities	26
Cooperation	26
<hr/>	
Annex: Resources	27
Glossary of Terms	28

Introduction: Building Canada's Information Economy and Society

Connecting Canadians

"We will make the information and knowledge infrastructure accessible to all Canadians by the year 2000, thereby making Canada the most connected nation in the world . . . A connected nation is more than wires, cables and computers. It is a nation in which citizens have access to the skills and knowledge they need to benefit from Canada's rapidly changing knowledge and information infrastructure. It is also a nation whose people are connected to each other."

Speech from the Throne,
September 23, 1997.

Canada's success in the 21st century depends increasingly on the ability of all Canadians to participate and succeed in the global, knowledge-based economy. And to ensure that success, all of us together — individual citizens, the private sector and governments at all levels — must move quickly to build Canada's information economy and society. For its part, the Government of Canada is committed to helping Canadians access the information and knowledge that will enable them, their communities, their businesses and their institutions, to find new opportunities for learning,

interacting, transacting and developing their economic and social potential.

That is what connecting Canadians is all about — discovering a world of economic and social opportunities by taking advantage of new technologies, information infrastructure, and multi-media content to spur business growth and development, create new and innovative jobs, improve our capacity to communicate directly with our fellow citizens and our public institutions and services, and extend our reach to other countries.

Electronic commerce, which is at the heart of the information economy, is the conduct of commercial activities and transactions by means of computer-based information and communications technologies. It generally involves the processing and transmission of digitized information. Examples of electronic commerce range from the exchange of vast amounts of financial assets between financial institutions, to electronic data interchange between wholesalers and retailers, to telephone banking, and to the purchase of products and services on the Internet.

For electronic commerce to flourish in Canada, it requires a clear, predictable and supportive environment where

citizens, institutions and businesses can feel comfortable, secure and confident. It also requires an international set of rules where citizens, institutions and businesses can easily exchange information, products and services across borders and around the world with predictable results and protection. This paper is one of a series related to electronic commerce which seeks your views on how to establish those clear and predictable rules that will make electronic commerce grow and thrive in Canada and will build Canada's information economy and society.

Protecting Personal Information

For Canada to become the most connected country in the world by the turn of the century, all of us — consumers, business and government — need to feel confident about how our personal information is gathered, stored, and used.

The challenge of the electronic age is that with each transaction we leave a data trail that can be compiled to provide a detailed record of our personal history and preferences. The digitization of health, education, employment and consumer records makes it possible to combine information and create an individual profile with data that most of us consider to be extremely personal. This information may be sent across provincial and national borders where it can be sold, reused

or integrated with other databases without our knowledge or consent.

As consumers and citizens, we need to know that when we shop or plan a vacation on the Internet, bank from home, look for work, correspond with friends and family, make purchases without cash using debit cards, find medical information or engage in other forms of electronic transactions, we have some control over our information and can be assured that it enjoys a basic level of protection.

The Government of Canada is committed to setting clear and predictable rules governing the protection of personal information.

In May 1996, responding to a recommendation by the Information Highway Advisory Council, the Minister of Industry announced that the federal government would develop legislation to protect personal information in the private sector. In September 1996, the Minister of Justice reiterated this commitment and stipulated the government's intent to legislate by the year 2000. The Ministers of Industry and Justice have been jointly charged with developing the legislation, in consultation with the provinces and territories and with other stakeholders.

Legislation that strikes the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that

information will be used and assured that the information will be protected is key to building the consumer trust and market certainty needed to make Canada a world leader in electronic commerce. At the same time, such legislation will provide our trading partners from around the world with the reassurance they need to engage in transactions that require cross-border transfers of personal information.

This discussion paper seeks your views on how to strike the right balance in the new legislation. It sets out the main issues that need to be addressed and outlines some options for the legislation, followed by some specific questions for your consideration. Your input is important; it will help ensure that the new legislation reflects a variety of interests while building the confidence of Canadians in electronic transactions.

Part 1: What is Privacy?

In repeated surveys, Canadians have expressed concern about privacy in general and about the loss of control over their personal information in particular. This kind of privacy is known as information privacy, and is defined as the right of individuals to determine when, how and to what extent they will share personal information about themselves with others.

Information privacy is important for a number of reasons. First, it is related to a series of other rights and values such as liberty, freedom of expression and freedom of association. Without some control over our personal information, our ability to enjoy these rights may be hindered.

Second, as more information about us becomes available, it is used in a wider variety of situations to make decisions about issues such as the kinds of services we are entitled to, the jobs we are qualified for and the benefits we may be eligible for. It is extremely important to have mechanisms in place to give us control over our own personal information and enable us to ensure that it is both accurate and relevant.

What Protection Exists Now?

The federal government and most provinces have legislation governing the public sector's collection, use and disclosure of personal information. The federal *Privacy Act* (1985) applies to all federal government departments, most federal agencies, and some federal Crown corporations. The Privacy Commissioner of Canada oversees the Act, and has powers to receive complaints, conduct investigations, and attempt to resolve disputes, among others. The Commissioner can also issue recommendations. Disputes about the right of access to personal information that are not resolved in this way can be taken to the Federal Court of Canada for judicial review.

The private sector is another matter. To date, only Quebec has adopted comprehensive privacy legislation for the private sector. Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* provides a detailed framework for the collection, use and disclosure of personal information. It is overseen by the Commission on Access to Information, which is responsible for conducting investigations and settling disputes.

In the rest of Canada, protection in the private sector is sporadic and uneven. Many industries are not

subject to any rules regarding the collection, use and disclosure of personal information, but a few are covered by what has been described by the Privacy Commissioner of Canada as a “patchwork” of laws, regulations and codes. The patchwork is made up of various federal and provincial laws, resulting in protection that is incomplete and possibly inconsistent. Effective as the patchwork may be in particular sectors, it does not establish common principles for all sectors and it does not cover all sectors. This incompleteness makes for uncertainty for business and a lack of uniform protection for consumers. And while the patchwork is useful as far as it goes, it is not adequate in the face of new developments.

Why Current Protection is No Longer Enough

New technologies, increasing data collection in the private sector, changing market trends and the new global marketplace for electronic commerce are contributing to the increasingly important role of information in the global economy. In the new global economy, information is a valuable commodity that can bring jobs, prosperity and higher levels of customer service. This, along with a number of other key factors, is creating mounting pressure to collect and use personal information more broadly than ever before.

In an environment where over half of Canadians agree that the information highway is reducing the level of privacy in Canada,¹ ensuring consumer confidence is key to securing growth in the Canadian information economy. Legislation that establishes a set of common rules for the protection of personal information will help to build consumer confidence and create a level playing field where the misuse of personal information cannot result in a competitive advantage.

One key factor leading to increased pressure on current protection is the advances in network browsers and sophisticated software that mean that information is no longer kept solely in central databases but can be distributed over all the networks of an organization. This makes conventional geographic borders less and less relevant. And whereas in older, paper-based records systems, segregation of information was the norm, new systems make it easy and affordable to combine information from many sources to create a profile or to make decisions.

Another factor is that the emphasis in legislation on information held by the public sector does not reflect the reality that the private sector is now a major collector and user of personal information. Historically, the concern has been that governments hold a great deal of information about citizens, and this has prompted legislative action to put limits on the uses to

1. Ekos Research Associates Inc., “Information Highway and the Canadian Communication Household, Draft Wave 1 Report,” January 1998.

which the information can be put and to provide citizens with opportunities to see and request correction of records about themselves. As we move increasingly into the information economy and society, however, and information itself becomes a commodity, the private sector is becoming an increasingly significant collector and user of personal information in the marketplace, and in third-party delivery of government services. It is important that this trend be reflected in new legislation that will ensure there are common guidelines for the handling and treatment of this information.

At the same time, the blurring of previously distinct market areas is another factor creating new pressures on existing rules and laws. For example, both cable and telephone companies now offer Internet access as part of their product line, as do many unregulated small businesses. Since these sectors are subject to different laws, this kind of convergence may create confusion for consumers about which rules apply to which companies, and under what circumstances, and whom they should complain to if there is a problem.

Some organizations have reacted positively to the privacy challenge and have developed voluntary codes to guide their collection and use of personal information. For example, the Canadian Direct Marketing Association requires its members to abide by a Code of Ethics that

includes rules about the collection and use of personal information. The problem, however, is that not all direct marketers belong to the association, and there is no mechanism for ensuring that they abide by the same rules. Not all businesses or industry associations have undertaken voluntary measures, and there may be a short-term incentive for some companies to ignore such measures and to use personal information inappropriately. This can undermine fair competition in the marketplace, creating an unlevel playing field. It can also erode consumer confidence in an entire industry and create further confusion about rights and rules.

The ability to provide effective protection for personal information may be crucial to Canada's ability to remain competitive internationally in the global information economy. For example, it may affect the exchange of data with European Union member states. In 1995, the European Union enacted a *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. The Directive is designed to harmonize data protection practices within the European Union. One of its requirements is for member states to adopt laws to protect personal information in both the public and private sectors. These laws must also include a provision to block transfers of information to non-member states that do not provide an "adequate" level of protection.

This Directive has the potential to make the protection of personal information a major non-tariff trade barrier with Canada. Failure to provide adequate protection for personal information may put Canada at risk of having “data flows” from the European Union blocked. Without comprehensive data protection legislation, Canadian businesses may be forced to undertake individual contractual negotiations to show compliance with the European Union rules. This process will be fraught with uncertainty and could become lengthy and expensive. It could also result in a higher standard of protection for information coming from outside the country than for information generated within our borders.

These and other pressures are likely to grow in the coming years. The global challenge to compete in the electronic commerce marketplace means that we do not have time for a slow, evolutionary approach to building up the protection of personal information and consumer trust. And citizens are also rightly asking for adequate protection in the new digital economy. It is therefore important to act now to develop legislation that will anticipate and adequately address both current and future challenges.

Protecting Personal Information: The Rules of the Road

Most efforts at legislating privacy begin with “fair information practices,” which are sets of privacy principles. Fair information practices are guidelines for the collection, use, disclosure, retention and disposal of personal information.

Sets of fair information practices vary, but they generally include the following principles:

- ensuring public awareness and transparency (openness) of information policies and practices
- establishing necessity and relevance of the information collected
- building in finality (establishing the uses of the information in advance and eventually destroying it)
- identifying the person who has responsibility for protecting personal information within an organization
- getting informed consent from the individual
- maintaining accuracy and completeness of records
- providing access to the information and a right of correction.

Fair information practices are the cornerstone of most efforts to protect personal information around the world. They form the basis of the

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were developed by the Organisation for Economic Co-operation and Development (OECD) in 1980 and signed by Canada in 1984. The Guidelines were designed both to protect personal information and to ensure the free flow of information.

These Guidelines have been widely adopted. Their influence can be seen in Quebec's legislation to protect personal information in the private sector. It is also apparent in the laws that govern the public sector federally, as well as in the provinces of British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec and Nova Scotia and the Yukon and the Northwest Territories. New Brunswick is preparing to introduce such legislation shortly.

The CSA Standard

While the current privacy protection regime in the private sector is clearly in need of refocussing, important work has been done in the past few years. In the early 1990s, the Canadian Standards Association (CSA) gathered representatives from the public sector, industries (including transportation, telecommunications, information technology, insurance, health, and banking), consumer advocacy groups, unions and other general-interest groups to discuss the need for a common code to protect personal information in the private sector.

The outcome of the initiative was the development of the Model Code for the Protection of Personal Information, which represents a consensus among all the stakeholders. Based on the OECD Guidelines, the Code is a set of principles for the protection of personal information in the private sector. It addresses two broad concerns: the way in which organizations collect, use, disclose and protect personal information; and the right of individuals to have access to personal information about themselves and to have the information corrected if necessary.

The Standards Council of Canada adopted the CSA Code as a National Standard in 1996, making Canada the first country in the world to adopt such a standard. The Standard demonstrates the continued commitment of participating parties to fair information practices, while providing an instrument that promises to be consumer-friendly, fair, effective and cost-efficient. The result of cooperation among a wide cross section of interest groups, it is truly a remarkable achievement.

The CSA Standard has generated significant international interest. In May 1996, the consumer policy group of the International Organization for Standardization (ISO) passed a unanimous, 25-country resolution in favour of a proposal to develop an international standard on privacy based on the CSA Standard. ISO is

now studying whether there is a need for an international standard to address information privacy, measure privacy protection and ensure global harmonization. If ISO accepts the CSA Standard as the basis for an international standard, Canadian companies that have already applied the principles of the Standard will have a significant advantage.

A few of the organizations that voted unanimously in support the CSA Model Code:

- American Express Company
- Cable Television Standards Foundation
- Canadian Bankers Association
- Canadian Cable Television Association
- Canadian Direct Marketing Association
- Canadian Labour Congress
- Canadian Life & Health Insurance Association
- Equifax Canada
- Fédération nationale des associations de consommateurs du Québec
- Information Technology Association of Canada
- Information Technology Industry Council
- Insurance Bureau of Canada
- Public Interest Advocacy Centre
- The Reader's Digest Association
- Stentor Telecom Policy Inc.

The success of the CSA Standard puts Canada in a good position to move forward from an environment of voluntary codes to a regulated approach to privacy protection. The new legislation will build on the work that has already been done to develop the Standard, as well as the work that various industries have done to implement it. By doing so, the legislation will address two fundamental issues. First, while the Standard provides solid protection, it is only a voluntary instrument, so there is no guarantee that it will be widely implemented. Legislation will ensure that the privacy principles are widely implemented, providing even protection for consumers. Second, as a voluntary instrument, the Standard does not provide for oversight or any way of ensuring effective consumer redress when there is a dispute. Light, flexible and effective legislation will provide the kind of backup that is needed to ensure that, when there are problems, consumers have mechanisms for recourse.

Part 2: Designing Canada's New Privacy Law

The second part of this paper looks at a series of issues that must be addressed in developing legislation to protect personal information in the private sector, and sets out some options for how these issues can be approached. In particular, the new legislation will need to address the four key elements common to all data-protection laws:

- obligations based on fair information practices
- administrative arrangements for an overseeing body to ensure accountability
- powers for overseeing authorities and judicial bodies
- powers and responsibilities that will promote public awareness and ensure effective implementation of obligations.

Throughout this section, the emphasis is on developing a legislative regime that draws on the best features of legislation in other countries and builds on the success of the CSA Standard.

Canada's new legislation should:

1. foster responsible privacy practices on the part of those in the private sector who hold personal information
2. provide light but effective guidance for protecting enforceable rights and

a level playing field in the marketplace, where personal information is an increasingly important element

3. be flexible, simple and effective, and consumer-friendly, with enforceable rights and effective means for redress
4. be cost-effective and administratively efficient and not overly burdensome for industry, especially small businesses
5. conform with our international obligations and trade agreements.

Ensuring Protection across Canada

In constructing a model for Canada, one of the fundamental considerations will be how the responsibility for protecting personal information in the private sector should be shared among the provincial, territorial and federal governments.

In Canada, some parts of the private sector are federally regulated, such as the telecommunications and banking industries and interprovincial transportation. Other parts of the private sector, such as health care and education, fall under provincial jurisdiction. Harmonized protection of personal information that covers the entire private sector would be the best way to address the increasing

mobility of information and to guard against the creation of “data havens” or barriers to the free flow of information.

If truly comprehensive privacy protection for all Canadians is to be achieved, then the federal, provincial and territorial governments will have to work closely and cooperatively to ensure a harmonized approach in all jurisdictions. This is vital for interprovincial trade, as well as for international trade.

One possible forum for such cooperation is the Uniform Law Conference of Canada (ULCC), an independent group that promotes the uniformity of legislation across the country. The ULCC began working on a draft Uniform Data Protection Act for the private sector in 1995, and expects to circulate a draft uniform Act for comments in 1998. Once complete, this model could help federal, provincial and territorial governments to develop a harmonized approach.

Other forums being used to work cooperatively on the protection of personal information across all jurisdictions are the Information Highway Ministers' Meetings and similar meetings of Consumer Affairs Ministers. These meetings are good opportunities for Ministers to identify common goals and to commit themselves to working in a harmonized fashion.

Finding Basic Principles

The first question in putting together legislation to protect privacy in the private sector is: What set of principles should the law be based on? Since the same basic set of fair information practices is found in legislation throughout the world, any of these could serve as the basis of the law. It would make sense, however, to build on the consensus that has been achieved around our National Standard. The CSA Standard has been acknowledged in many forums as an improvement over the OECD Guidelines. Principles based on the CSA Standard would help to ensure compatibility with other regimes that have also legislated to a higher standard than the Guidelines, such as Quebec.

The Standard embodies the following 10 fair information principles:

- **Accountability:** An organization is responsible for personal information under its control, and shall designate an individual or individuals who are accountable for the organization's compliance with the Code's principles.
- **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
- **Consent:** The knowledge and consent of the individual are required for the collection, use

or disclosure of personal information, except where inappropriate.

- **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
- **Limiting Use, Disclosure and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as is necessary for the fulfilment of those purposes.
- **Accuracy:** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
- **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- **Individual Access:** Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able

to challenge the accuracy and completeness of the information and have it amended as appropriate.

- **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The CSA Standard includes an interpretation of each of the 10 principles. There is also a companion workbook that provides more detailed guidance on putting the Standard into practice. These tools make it easy for companies to interpret and implement the Standard.

The CSA Standard has a number of advantages as a starting point for legislation. First, it represents a consensus among key stakeholders from the private sector, consumer and other public interest organizations, and some government bodies. Second, the CSA Standard provides flexibility; it was designed to serve as a model for more specific industry codes. Third, the CSA Standard is technologically neutral; its principles go beyond specific industry applications. Consequently, the Standard will not become outdated as technologies for the collection and storage of information change. Ideal legislation for Canada would build on the successes in voluntary compliance experienced with the CSA Standard while ensuring its rapid, widespread implementation.

If the legislation were to be based on the CSA Standard, a number of questions would have to be addressed.

To begin with, is the CSA Standard, which was drafted as a voluntary instrument, precise enough in setting out legal obligations or would it require further elaboration? Precision and certainty are important aspects of any legislation, because they help ensure that governments, consumers and businesses are clear on their respective rights and responsibilities. Such clarity is especially important when a dispute between an individual and an organization may have legal implications. Provisions of the CSA Standard that may need to be made more precise include when and how personal information may be collected and for what reasons, how long an organization may keep such information, what consent must be obtained for its collection and in what form, and what fees can be charged for copies of records.

The law would also have to specify the exceptional circumstances under which personal information may be disclosed to a third party without the consent of the individual. Sometimes these disclosures do not fall within the purposes for collection as stated by the organization. Such circumstances might include the protection of the health and safety of one or more individuals, emergency situations where it

is impossible to obtain the individual's consent, the conduct of medical research, the compilation of statistics, the conduct of lawful investigations, and compliance with a court order.

A second question is: Are there any additional obligations not set out in the CSA Standard that should be included in the legislation? Such obligations could include a duty to report any complaints received to a government body or a requirement to educate members of the public about their rights, or indeed new obligations unforeseen in the original Standard.

A third question is: should some types of information be excluded from the scope of the legislation? For example, Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* does not apply to journalistic material collected, held, used or communicated for the purpose of informing the public.

At a technical level, the obligations and approach of the CSA Standard could be incorporated in law by setting out the basic principles in the statute, with more precise details included in regulations or some other instrument such as sectoral codes. Regardless of how the necessary details were incorporated into law, organizations that use personal information would be required to meet the obligations of the statute.

Sectoral Codes

Many organizations in Canada have already developed privacy codes, and some are upgrading them to meet the CSA Standard. The Canadian Bankers Association, the Insurance Bureau of Canada and the Cable Television Standards Foundation, for instance, have already released codes that conform to the Standard. Other organizations are also working toward this goal.

Sectoral and company codes provide detail and guidance on how legal requirements apply to a specific industry or company. In some ways, these codes are a blueprint for how the law will be reflected in the real-life information practices of the companies that are subject to them.

Many organizations may find that the principles of the legislation are sufficient in themselves, and may not feel a need to develop their own specific codes. This is likely to be the case for many small businesses. Such organizations would simply be required to adhere to the principles set out in the law. Other organizations, however, may prefer to draw on their

own expertise to interpret the law as it relates directly to their line of business, and so may see value in developing sectoral codes which would supplement or replace the requirements of the law.

Sectoral codes can be beneficial in a number of ways. First, they allow industries to explore their own needs for personal information and to show their commitment to privacy by imposing discipline on their own practices. This commitment and leadership can help create consumer trust, and they encourage both consumer protection and market leadership. Second, the process of developing a code can help to promote education and acceptance of good information management practices within an organization, thus encouraging staff and management to take an active approach to interpreting and implementing their own information practices. Third, the existence of specific codes facilitates audits by providing a manual of information practices, which can be used as a measuring stick against which to judge the practices of particular companies.

Sectoral Codes in Practice: The Canadian Bankers Association Privacy Model Code

The Canadian Bankers Association (CBA) has been a leader in developing voluntary approaches to protecting personal information. The banking industry developed its first privacy code in 1986, and modified it subsequently on two occasions. Then, over the period 1995–1996, the CBA worked to ensure that its code was consistent with the CSA Standard.

The CBA code has been verified as complying with the CSA Code by Price Waterhouse, and banks are now working individually toward full implementation of the provisions of the code through their own privacy codes.

Copies of the CBA code are available from:

Canadian Bankers Association
Box 348, Commerce Court West
30th Floor
Toronto ON M5L 1G2

Tel.: (416) 362-6092
Fax: (416) 362-7705

Recognition of Sectoral Codes

Should sectoral codes be recognized in the new law? If so, should they be binding, or should they be used only to help guide the interpretation of the principles of the law for specific sectors?

Other jurisdictions have dealt with these issues in a variety of ways. The Quebec law, for example, makes no reference to sectoral codes. Nevertheless, several industry associations with members operating in Quebec have developed such codes for their own organizational purposes.

The United Kingdom law obliges the Data Protection Registrar to encourage the development of codes. These codes aid in interpreting the law, but are not legally binding. The law in the Netherlands makes the Privacy Commissioner responsible for approving codes developed by industry. As in the United Kingdom, these codes are not binding but do give guidance in interpreting the law.

In New Zealand, sectoral codes have the full force of law. A code may be more or less stringent than the principles set out in the law but, once it has been approved by the Privacy Commissioner, it replaces those principles. Developing such codes is a labour-intensive process, but has resulted in a very thorough Code for the Protection of Health Information and one for the use of unique identifying numbers for superannuation.

There are essentially two ways of recognizing sectoral codes in the law:

- Building on the Netherlands approach, industries could be encouraged to tailor codes. Once approved, the codes would be used to guide interpretation but would not be legally binding.
- Following the New Zealand model, approved codes could replace the requirements set out in the legislation and be legally binding.

A further question arises from these options: Who should develop sectoral codes? Having industry develop the codes would avoid placing a huge burden on government overseeing agencies, which generally would be ill-placed to develop specific sectoral guidelines on their own but which are most useful in engaging companies in a dialogue about the adequacy of the finished product. To assist them in developing codes, companies could make use of the growing body of privacy expertise. Alternatively, a government body with privacy expertise could take on the task of developing the codes.

Approval

Once sectoral codes have been written, who should approve them and how?

Legally binding codes clearly require a more rigorous process than codes that would simply provide guidance. Care must be taken to avoid setting up

a conflict-of-interest situation whereby a privacy commissioner, for instance, would collaborate on the development of a code and then be tasked with resolving consumer complaints about it.

Regardless of whether or not the codes are binding, they could be approved through a government body responsible for verifying each code to make sure it conforms with the law. This body could then conduct an audit of organizations implementing the code to assess the level of conformity and approve the code. Administrative or legal measures would have to be put in place to ensure that, if the same body had overseeing powers, no conflict of interest would arise. The cost of having such a body approve codes, from the point of view of both government and industry, must be weighed against the possible costs associated with other methods of approving codes.

Non-binding codes could also be verified by either:

- a body accredited as a quality registrar by the Standards Council of Canada, which would conduct an information audit, as is the case now with the process of registering to the CSA Standard; or
- internal or external auditors or other parties with expertise in information management.

Binding codes could also be verified in one of two ways:

- By an accredited registrar. The registrar would recommend that the code be recognized as conforming with the law. A government body or official would receive the recommendation, hold open public hearings, and give the final approval for verification.
- By a government oversight body. Following verification by that body, an approved auditor would conduct an information audit to ensure that the code is being implemented. After the audit, companies could apply for a ministerial exemption allowing them to replace the requirements of the law with their own sectoral codes. There could be provisions for public comment before the code is approved, and passing periodic audits would be necessary to maintain the exemption.

Ensuring Compliance with the Law and Effective Redress of Complaints

Once the basic obligations and the role of sectoral codes have been clarified, their compliance must be assured through an overseeing regime for handling complaints and resolving disputes. Another function of the oversight regime would be ensuring that both the public and the organizations affected by the law are aware of and adhere to its provisions.

Most existing laws for the protection of personal information in jurisdictions around the world establish one central

oversight authority, but this varies, particularly in federal states. It would probably make sense to use existing oversight bodies where appropriate, such as the Office of the Privacy Commissioner of Canada.

In designing the most appropriate oversight regime for Canada, there are two primary considerations. The first is the powers needed to adequately oversee observance of the new law and ensure redress. The second is how these powers should be distributed.

It is important to keep in mind that certain kinds of powers, such as ordering fines or restitution when the law is violated, are appropriate to some oversight bodies but not to others. Given appropriate powers and responsibilities, industry associations, existing regulatory and self-regulatory bodies, a privacy commissioner and a federal court or tribunal all could play a role in overseeing privacy protection. In determining who makes final decisions, possible conflicts of interest must be guarded against.

Accountability

The first issue anyone charged with overseeing the new legislation must address is: Are the people and organizations complying with the law? The CSA Standard requires that companies identify an officer within the organization who will be accountable for compliance. This obligation would become binding in the new law. Additional mechanisms could also be

used to ensure compliance with the new law, such as the following examples:

- some kind of registration requirement that organizations state their information management practices, as in the system in the United Kingdom
- some kind of initial audit to ensure adherence to the law
- encouragement, if not a requirement, for organizations to undergo some sort of external review of their information management practices to demonstrate their compliance
- reliance solely on complaints to expose violations
- reliance on a central authority with broad powers to conduct research, write reports, and conduct investigations.

Registration and audit schemes have value in that they help identify problems early on in the implementation process. They also serve to educate staff within an organization. A scheme whereby external review is compulsory could have some drawbacks, however. It may place a heavy burden on small businesses and on organizations that make little use of personal information or of information that is sensitive. It may also be expensive and burdensome to government.

It may be more viable for government to encourage, but not require, organizations to have their information

practices audited. In this way, companies could show market leadership and demonstrate a greater commitment to privacy. One way to do this could be by permitting formal registration to the CSA Standard through a body accredited by the Standards Council of Canada. This approach would build on existing mechanisms and current voluntary practices. Companies choosing not to undergo such audits would still have to comply with the law, however.

Another option would be to neither require nor encourage any registration or third-party appraisal of information management practices. In many countries with data-protection laws, compliance is assumed unless a dispute or investigation reveals a problem. A possible weakness of this approach is that it relies heavily on the public to discover abuses, which can be quite difficult in the current climate of sophisticated dataprocessing techniques.

To compensate for this potential weakness, the law could deal with compliance monitoring by empowering a central authority or privacy commissioner to do research, prepare reports on new issues such as new technologies, and perform audits or inspections proactively in addition to responding to complaints. In order for this to be as effective as an upfront registration or audit scheme, there would have to be significant resources committed to this function.

Response to Complaints

The next issue is the handling of complaints. The legislation will give individuals the right to complain and to challenge compliance with any part of the law, affording them a key role in monitoring organizations. By directing the complaint to the company first, a potentially significant burden on the oversight authority is reduced.

Thus, businesses will have the opportunity to learn from their mistakes and show market leadership in correcting them and developing consumer trust.

Businesses should take an active role in monitoring their own practices and should cooperate with consumers in resolving problems. To help track compliance with the law, companies could be required to report any complaints they receive to an oversight body.

In the event that an individual is not satisfied with an organization's accountability mechanisms, however, there must be a second avenue for redress. The oversight body should have a range of powers to investigate and to attempt settlement. It should be able either to reach final judgment on the dispute or to empower the individual to move on to a court for final judgment.

Several questions arise:

- What powers are needed to investigate possible cases of

non-compliance and resolve disputes? These could include the power to receive and initiate complaints, investigate information practices, conduct or demand an audit, examine witnesses, require testimony and order the production of documents, act as a mediator in disputes, and issue recommendations or binding orders.

- What powers are needed to address violations of the law and compensate individuals who have been harmed? These could include powers to order fines or restitution, award damages, order corrective action, demand full registration to the CSA Standard if the law does not already require it, order periodic audits, restrict the use or transfer of personal information by non-compliant companies, and publish the details of violations.

Oversight Agencies

An important aspect of any legislation to protect privacy in the private sector is the mechanism by which effective oversight of the law is ensured. There are a number of agencies which could be used to perform this function. For example, in Canada, banks, cable companies, airlines and other industries are already subject to the authority of regulatory agencies. These agencies have expertise in these industries, so it would make sense to use existing regulatory bodies in some capacity for overseeing privacy protection. Care

should be taken, however, to ensure that taking on this additional capacity would not weaken the coherence of a harmonized regime or result in differing interpretations of the legislation.

There may be value in distributing the oversight powers among a number of agencies, which could include businesses, industry associations and existing regulatory bodies in conjunction with a privacy commissioner or a special court or tribunal. The distribution of powers among these agencies could be determined on the basis of existing practices, cost, conflict of interest and recognition of the fundamental rights of the individual to effective redress.

The first step in any normal redress procedure could be consideration of the complaint by the company involved. If the problem is not resolved, the complaint could then go to the privacy commissioner, who could mediate or refer the complaint back to the company for mediation through industry-led mechanisms, assuming these have not already proven unsuccessful. Such mechanisms might include an industry ombudsman or some other body. In several sectors, such as banking or telecommunications and broadcasting, regulatory bodies could play a role.

Where disputes deal with systemic issues or where complainants do not feel that they can obtain satisfaction through industry-led processes, there

may be a role for the privacy commissioner, a special court or tribunal, or both. Extending the mandate of the existing Privacy Commissioner would require additional resources, but some of the functions normally associated with the Commissioner could be distributed among the various other parties.

A privacy commissioner with a mandate to monitor compliance, make recommendations about sectoral codes and issue special reports on new technologies or practices might be compromised in having to make a final binding judgment on a complaint involving activities he or she had overseen or audited. Several other countries have set up special tribunals for hearing cases to avoid this situation. Does this option have merit for Canada?

Public Education

Legislation to protect privacy in the private sector would be most effective if it included measures that address emerging privacy issues proactively through consumer education. In a light regulatory framework which does not impose a heavy burden on industry, consumer education is especially important to ensure that citizens are well informed about their privacy rights and are vigilant in protecting them.

The following issues need to be considered:

- Where should responsibility for public education lie? The law could make the privacy commissioner solely responsible, or it could divide the responsibility with businesses, industry associations and regulatory bodies.
- Should the privacy commissioner be encouraged or required to provide advice to individual companies on privacy issues? This could be done informally or in conjunction with compliance audits. In many countries, including Canada, privacy commissioners provide advice to organizations about their information management practices and about privacy issues more generally, through both informal and formal channels. This gives the commissioners an opportunity to influence systems at the design stage, and helps to raise awareness of and sensitivity to privacy issues. Providing this kind of advice must not, however, interfere with the commissioners' ability to receive complaints or conduct investigations.
- Should the law require privacy impact assessments of new information technologies? If so, when and by whom? New information technologies can either erode or preserve privacy. The legislation could play a role in promoting the use of those that enhance privacy by requiring privacy impact assessments of all

new information technologies where appropriate. These assessments would focus on how the new information technology protects personal privacy, whether it provides more or less protection than previous technologies for the same purpose, and whether it provides options, such as paying for services anonymously, for individuals who demand greater privacy.

Striking the Right Balance for Made-in-Canada Legislation

The challenge facing Canadians is to find a balance between the needs of business for access to the information necessary for functioning in a knowledge-based economy and the rights of individuals to privacy and security of personal information. Collectively, we must ensure that technological innovations do not become intrusions on these economic needs and fundamental rights. Because the information economy is still in its infancy, Canadians now have the opportunity to define and design the kind of system we want to establish for safeguarding information privacy in the private sector. Rapid technological advances, however, demand that we formulate a legislative framework before many of the issues discussed in this paper move beyond our control.

Even in dealing with such a complex issue as protection of personal information in a digital economy and society, it is possible for citizens, businesses, and governments to reach a common understanding and to find a solution which addresses the needs of all stakeholders. The CSA Standard

is an excellent case in point. This discussion paper will encourage public debate on the issues it lays out, and submissions in response to the paper will contribute to the formulation of a common Canadian approach to the protection of personal information in the private sector.

Part 3: Your Turn

This paper has raised a number of specific questions with regard to the form that federal legislation to protect privacy in the private sector should take. In considering these questions, it is important to make sure that the new law strikes the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that information will be used and assured that the information will be protected. Achieving this balance is a key element in fostering an environment that will enable Canada to emerge as a world leader in electronic commerce.

Industry Canada and Justice Canada look forward to receiving your comments on the questions raised throughout the paper. For your convenience they are listed below, along with some related questions that will also need to be addressed as we develop legislation.

Obligations

1. Is the CSA Standard the base from which to start in drafting legislation? Is it precise enough in setting out obligations or do some obligations require further elaboration? Are there any additional obligations not set out in the CSA Standard that should be included in the legislation?
2. Under what circumstances should the law permit disclosure of personal information to a third party without the consent of the individual? What conditions should apply?
3. Should sectoral codes be recognized in the new law? If so, should they be binding? Or should they be used only to help interpret the principles of the law for specific sectors? Who should develop and approve them?
4. Should some types of information be excluded from the scope of the legislation? If so, in what circumstances?

Powers

5. Do you favour start-up obligations such as a registration scheme to ensure compliance with the law? If so, which approach do you favour? Who should be responsible for overseeing privacy protection?

6. What powers are needed to investigate possible cases of non-compliance and resolve disputes about the terms of compliance?

7. What powers are needed to address violations of the law and compensate individuals who have been harmed?

8. Should there be powers to conduct independent research and proactive investigation/inspection of an organization's practices and to write reports?

Distribution of Powers and Responsibilities

9. Should a central oversight authority be established to oversee the implementation of the new legislation, and if so, what powers should it have? Should this role be added to the responsibilities of the federal Privacy Commissioner or some other body?

10. Should a tribunal be established, or should a higher court be given the task of issuing binding decisions on complaints?

11. What use should be made of existing industry regulators or of industry-led, self-regulatory mechanisms? How can such bodies be set up to satisfy business, consumer and government expectations?

12. How should responsibilities for public education be assigned?

13. Should the law require privacy impact assessments of new technologies? If so, when and by whom?

Cooperation

14. How should responsibilities for protecting personal information in the private sector be shared among the provincial, territorial and federal governments?

15. What forums, in addition to those discussed in the paper, would be useful in harmonizing the protection of personal information in all jurisdictions in Canada?

Thank you for your contribution to this consultation process. Please have your responses in by March 27, 1998. Send your comments to:

Helen McDonald
Director General, Policy Development
Task Force on Electronic Commerce
Industry Canada
20th Floor, 300 Slater Street
Ottawa ON K1A 0C8
Fax: (613) 957-8837
E-mail: privacy@ic.gc.ca

Annex: Resources

A number of publications are referred to in this paper. Many of them are available electronically, and paper copies can be obtained by contacting the Industry Canada Task Force on Electronic Commerce:

Tel.: (613) 990-4255

Fax: (613) 957-8837

E-mail: privacy@ic.gc.ca

CAN/CSA-Q830-96 Model Code for the Protection of Personal Information (the CSA Standard) is available at: <http://www.csa.ca/83002-g.htm>

The 1980 **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, developed by the Organisation for Economic Co-operation and Development (OECD), an abridged version are available at: <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM#3>

The 1995 European Union **Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data** is available at: <http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html>

The federal **Privacy Act** is at: <http://canada.justice.gc.ca/stable/EN/Laws/Chap/P/P-21.html>

Two excellent sources of further on-line information about privacy are:

The **Office of the Privacy Commissioner of Canada**, at: <http://infoweb.magi.com/~privcan/>

Media Awareness Network, at: <http://www.schoolnet.ca/medianet>

Glossary of Terms

A number of terms are used throughout this paper which have a specific meaning within the context of privacy and the protection of personal information. They are listed below.

Electronic Commerce: All commercial transactions, involving organizations and/or individuals, based on the processing and transmission of digitized information.

Information Privacy: A subset of privacy, it involves the right of individuals to determine when, how and to what extent they will share personal information about themselves with others. Protecting information privacy involves protecting personal information.

Personal Information: Any information about an identifiable individual that is recorded in any form, including electronically or on paper. Some examples would be information about a person's religion, age, financial transactions, medical history, address, or blood type.

Privacy: Most often defined as the right to be left alone, free from intrusion or interruption, privacy is an umbrella term, encompassing elements such as physical privacy, communications privacy, and information privacy. Privacy is linked to other fundamental human rights such as freedom and personal autonomy.

Glossaire

Plusieurs termes utilisés dans le présent document ont une signification particulière dans le contexte de la vie privée et de la protection des renseignements personnels. En voici une liste.

Commerce électronique : Toutes les transactions commerciales auxquelles sont parties des organisations ou des personnes, reposant sur le traitement et la transmission d'information numérisée.

Protection des renseignements

personnels : Ce sous-ensemble du respect de la vie privée comprend le droit des personnes à déterminer

quand, comment et dans quelle mesure elles souhaitent partager avec autrui des renseignements personnels. La protection de la vie privée passe par la protection des renseignements personnels.

Renseignements personnels : Tous les renseignements se rapportant à une personne identifiable qui est enregistré, quels que soient leur forme et leur support, y compris électronique ou sur papier. Il peut s'agir de la religion ou de l'âge d'une personne, ses opérations financières, son histoire médicale, son adresse ou son groupe sanguin.

Vie privée : La vie privée, qui se définit souvent comme le droit à la tranquillité, celui de ne pas subir d'intrusion, est une expression générale qui recouvre des éléments tels que la vie privée au sens matériel, le secret des communications et la protection des renseignements

personnels. Le respect de la vie privée est lié à d'autres droits fondamentaux de la personne tels que la liberté et l'autonomie personnelle.

Annexe : Documents de référence

Le présent document comporte des références à plusieurs publications. Nombre d'entre elles existent en version électronique, et il est possible de s'en procurer des exemplaires imprimés en communiquant avec le Groupe de travail sur le commerce électronique d'Industrie Canada :

Téléphone : (613) 990-4255
Télocopieur : (613) 957-8837
Courrier électronique : vieprivée@ic.gc.ca

Vous trouverez le document intitulé **CAN/CSA-9830-96 Code type sur la protection des renseignements personnels** (la norme de la CSA) à l'adresse électronique suivante : <http://www.ca.ca/83002-g.htm>

Les **Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel** publiées en 1980 par l'Organisation de coopération et de développement économiques (OCDE) sont diffusées à l'adresse électronique suivante : <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM#3>

Pour consulter la **Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données** publiée par l'Union européenne en 1995, consultez l'adresse suivante : <http://www2.echo.lu/legal/fr/datapro/directiv/direct.html>

La **Loi sur la protection des renseignements personnels** du gouvernement fédéral se trouve à l'adresse électronique suivante : <http://canada.justice.gc.ca/FTP/FR/Lois/Chap/P-P-21>

De plus, vous voudrez sans doute consulter ces deux sources de renseignements en direct sur la protection des renseignements personnels :

le **Commissariat à la protection de la vie privée du Canada**, à <http://infoweb.magi.com/~privcan/>

Réseau éducation-médias, à <http://www.rescol.ca/medianeet>

13. La loi doit-elle prévoir l'évaluation des incidences des nouvelles technologies? Dans l'affirmative, quand et par qui?

Coopération

14. Comment les gouvernements fédéral, provinciaux et territoriaux doivent-ils se répartir les responsabilités en ce qui concerne la protection des renseignements personnels dans le secteur privé?

15. Quelles instances, en plus de celles dont il est question dans le présent document, peuvent contribuer à l'harmonisation de la protection des renseignements personnels à tous les paliers de gouvernement au Canada?

Nous vous remercions de votre contribution à ce processus de consultation. Vous pouvez nous faire parvenir vos commentaires jusqu'au 27 mars 1998; veuillez les adresser à :

Helen McDonald

Directrice générale
Développement des politiques
Groupe de travail sur le
commerce électronique
Industrie Canada

20^e étage, 300, rue Slater
Ottawa (Ontario) K1A 0C8
Télocopieur : (613) 957-8837
Courrier électronique :
vieprivée@ic.gc.ca

7. Quels sont les pouvoirs nécessaires pour sanctionner les infractions à la loi et dédommager les personnes qui ont subi un préjudice?

8. Faut-il habiliter quelqu'un à mener des recherches indépendantes et une enquête ou une inspection préventives sur les pratiques d'une organisation, et à rédiger des rapports?

Répartition des attributions

9. Faut-il créer une autorité centrale qui sera chargée de superviser la mise en œuvre de la nouvelle loi et, dans l'affirmative, quelles doivent en être les attributions? Ces attributions doivent-elles s'ajouter à celles du Commissaire à la protection de la vie privée ou d'un autre organisme?

10. Faut-il créer un tribunal ou charger une cour supérieure de rendre des décisions exécutoires suite à des plaintes?

11. Quel doit être le rôle des organes de réglementation de l'industrie et des mécanismes sectoriels d'autoréglementation existants? Quelles doivent être les attributions de ces organes s'ils doivent répondre aux attentes des entreprises, des consommateurs et des gouvernements?

12. Qui faut-il charger de l'éducation du public?

Partie 3 : La parole est à vous

Un certain nombre de questions précises sont posées dans le présent document quant à la forme que devrait prendre la loi fédérale sur la protection des renseignements personnels dans le secteur privé. Il est important, en les étudiant, de faire en sorte que la nouvelle loi trouve le bon équilibre entre la nécessité pour les entreprises de réunir, conserver et utiliser des renseignements personnels et le besoin des consommateurs de savoir comment ces renseignements seront utilisés et d'avoir l'assurance qu'ils seront protégés. Il est essentiel de trouver cet équilibre, si l'on veut instaurer un environnement qui permettra au Canada de jouer un rôle de premier plan dans le commerce électronique mondial.

Industrie Canada et Justice Canada attendent vos commentaires sur les questions soulevées tout au long du document. Pour vous aider, ces dernières ont été résumées ci-dessous, en plus des questions connexes auxquelles il faudra également répondre durant l'élaboration de la loi.

Obligations

1. La norme de la CSA doit-elle servir de point de départ à la rédaction de la loi? Est-elle assez précise dans l'énoncé des obligations ou faut-il apporter des éclaircissements? Y a-t-il

d'autres obligations que celles figurant dans la norme de la CSA et qui devraient figurer dans la loi?

2. Dans quelles circonstances la loi doit-elle permettre la divulgation de renseignements personnels à une tierce partie sans le consentement de l'intéressé? Quelles conditions devraient s'appliquer?

3. La nouvelle loi doit-elle reconnaître les codes sectoriels? Dans l'affirmative, doivent-ils avoir force exécutoire? Ou doivent-ils seulement aider à interpréter les principes de la loi pour des secteurs particuliers? Qui doit les élaborer et les approuver?

4. Faut-il exclure certains types de renseignements du champ d'application de la loi? Dans l'affirmative, dans quelles circonstances?

Pouvoirs

5. Êtes-vous favorable à des obligations initiales telles qu'une inscription destinée à garantir le respect de la loi? Dans l'affirmative, quelle méthode préférez-vous? Qui doit être chargé de surveiller la protection des renseignements personnels?

6. Quels sont les pouvoirs nécessaires pour faire enquête sur des cas éventuels de non-respect et pour régler des différends portant sur les conditions de la conformité avec la loi?

Arriver à un juste équilibre dans la loi canadienne

évaluation porterait essentiellement sur ce qui, dans la nouvelle technologie, protège la vie privée, plus ou moins que des technologies antérieures utilisées à la même fin, et verrait si elle propose des options, comme les paiements anonymes, aux personnes qui exigent plus de confidentialité.

Le défi pour les Canadiens consiste à trouver un équilibre entre la nécessité pour les entreprises d'avoir accès à des renseignements indispensables pour fonctionner dans une économie du savoir, et les droits des particuliers à la protection de la vie privée et à la sécurité des renseignements les concernant. Ensemble, nous devons veiller à ce que les innovations technologiques n'empêchent pas sur ces besoins économiques et ces droits fondamentaux. Parce que l'économie de l'information en est encore à ses balbutiements, les Canadiens ont la chance de pouvoir définir et concevoir

le type de régime qu'ils souhaitent mettre en place pour garantir la protection des renseignements personnels dans le secteur privé. Toutefois, les technologies progressant rapidement, nous devons tracer un cadre législatif avant que nous n'échappions à la maîtrise de nombre des questions examinées dans le présent document. Même face à un problème aussi complexe que celui de la protection des renseignements personnels dans une économie et une société fondées sur l'information, les citoyens, les entreprises et les gouvernements peuvent parvenir à s'entendre et à trouver une solution qui réponde aux besoins de tous les intervenants. La norme de la CSA est un excellent exemple à cet égard. Le présent document de travail encouragera le public à débattre les questions qui y sont posées et les soumissions reçues en réaction à ce document contribueront à définir au Canada une démarche commune en ce qui concerne la protection des renseignements personnels dans le secteur privé.

relative à des activités qu'il a surveillées ou vérifiées. Pour éviter cette situation, plusieurs autres pays ont chargé des tribunaux créés spécialement d'entendre les causes. Cette solution est-elle valable au Canada?

Educación du public

La loi visant à protéger les renseignements personnels dans le

secteur privé sera des plus efficaces si

elle comprend des mesures d'éducation

des consommateurs qui éviteront de

nouveaux problèmes. Dans un cadre

de réglementation souple qui n'impose

pas de lourd fardeau à l'industrie,

l'éducation des consommateurs revêt

une importance toute particulière,

car elle permet de faire en sorte que

les citoyens soient bien informés de

leurs droits à la vie privée et veillent

à les protéger.

Les questions suivantes devront être

examinées :

- Qui devrait être chargé de l'éducation du public? La loi pourrait prévoir que cette tâche incombe au seul Commissaire à la protection de la vie privée ou en partager la responsabilité entre les entreprises, les associations professionnelles et les organes de réglementation.
 - Faut-il encourager le Commissaire à la protection de la vie privée à conseiller les entreprises en matière de renseignements personnels
- des incidences des nouvelles technologies de l'information? Dans l'affirmative, quand devra-t-elle avoir lieu et qui en sera chargé? Les nouvelles technologies de l'information peuvent soit nuire à la protection des renseignements personnels soit la renforcer. La loi peut contribuer à inciter à utiliser les technologies qui préservent la vie privée en exigeant, si nécessaire, l'évaluation des incidences de toute nouvelle technologie de l'information sur la protection des renseignements personnels. Cette

- La loi doit-elle prévoir l'évaluation des incidences des nouvelles technologies de l'information? Dans l'affirmative, quand devra-t-elle avoir lieu et qui en sera chargé? Les nouvelles technologies de l'information peuvent soit nuire à la protection des renseignements personnels soit la renforcer. La loi peut contribuer à inciter à utiliser les technologies qui préservent la vie privée en exigeant, si nécessaire, l'évaluation des incidences des nouvelles technologies de l'information sur la protection des renseignements personnels. Cette
- ou bien l'y obliger? Ces conseils pourraient être officiels ou être prodigués parallèlement aux vérifications de conformité. Dans beaucoup de pays, dont le Canada, les commissaires à la protection de la vie privée conseillent les organisations au sujet de leurs pratiques en matière de gestion de l'information et sur les questions de protection des renseignements personnels, plus généralement, à titre officiel et officieux. Ils ont ainsi la possibilité d'influer sur les systèmes à l'étape de la conception, et ils contribuent à accroître la sensibilisation aux questions relatives à la protection des renseignements personnels. Cependant, dispenser ce genre de conseils ne doit pas empêcher les commissaires de recevoir des plaintes ou de mener des enquêtes.

Organismes de surveillance

Le mécanisme qui permet de surveiller l'application de la loi est un aspect important de toute loi destinée à protéger la vie privée dans le secteur privé. Plusieurs organismes pourraient assumer cette fonction. Par exemple, au Canada, les banques, les compagnies de cablodistribution, les lignes aériennes, notamment, relèvent déjà d'organes de réglementation qui connaissent ces industries. Il serait donc logique de leur confier un rôle dans la surveillance de la protection des renseignements personnels. Il faudrait veiller, toutefois, à ce que cette capacité supplémentaire n'entraîne pas la cohérence d'un régime harmonisé ou n'entraîne pas d'interprétations divergentes de la loi.

Il peut être bon de répartir les pouvoirs de surveillance entre un certain nombre d'organismes qui pourraient comprendre des entreprises, des associations professionnelles et des organes de réglementation existants, travaillant en liaison avec un commissaire à la protection de la vie privée ou avec une cour ou un tribunal spécial. Les critères suivants pourraient aider à la répartition des pouvoirs : les pratiques actuelles, le coût, les conflits d'intérêts possibles et le droit fondamental à un recours efficace.

La première étape dans toute procédure de recours devrait être que l'entreprise concernée examine la plainte. Si le problème n'est pas réglé, la plainte pourrait alors être portée

devant le Commissaire à la protection de la vie privée. Ce dernier pourrait servir de médiateur ou renvoyer la plainte à l'entreprise pour une médiation par le biais de procédés propres à l'industrie, à moins que l'entreprise n'ait déjà eu recours, sans succès, à ces procédés. Ces mécanismes peuvent comprendre l'intervention d'un ombudsman ou d'un organe sectoriel. Des organes de réglementation pourraient jouer un rôle dans plusieurs secteurs, comme dans les secteurs financiers ou dans les télécommunications et la radiodiffusion.

Lorsque les différents portent sur des problèmes systémiques ou lorsque les plaignants n'ont pas l'impression qu'ils peuvent obtenir gain de cause par le biais de processus sectoriels, le Commissaire à la protection de la vie privée, une cour ou un tribunal spécial ou les deux ont peut-être un rôle à jouer. Pour élargir le mandat actuel du Commissaire à la protection de la vie privée, il faudrait des ressources supplémentaires, mais certaines fonctions normalement associées au Commissaire pourraient être réparties entre les diverses autres parties.

Un commissaire à la protection de la vie privée chargé de veiller à la conformité, de formuler des recommandations sur les codes sectoriels pourrait se compromettre en ayant à rendre un jugement exécutoire et sans appel consécutif à une plainte

à trancher le litige de façon définitive, à autoriser le particulier à demander un jugement définitif à un tribunal.

Plusieurs questions se posent :

- Quels sont les pouvoirs nécessaires pour enquêter sur des cas éventuels de non-respect et pour régler des différends? Cela pourrait comprendre le pouvoir de recevoir des plaintes et de déposer plainte, d'enquêter sur les pratiques en matière d'information, de procéder à une vérification ou d'en demander une, d'interroger des témoins, de solliciter la production de documents, de servir de médiateur dans les différends, et d'émettre des recommandations ou des ordonnances exécutoires.

- Quels sont les pouvoirs nécessaires pour sanctionner les infractions à la loi et dédommager les personnes qui ont subi un préjudice? Il peut s'agir d'être habilité à infliger des amendes ou à ordonner une restitution, à accorder des dommages-intérêts, à exiger l'adhésion complète à la norme de la CSA, si la loi ne l'exige pas déjà, à ordonner des vérifications périodiques, à limiter l'utilisation ou le transfert de renseignements personnels par les entreprises en infraction, et à publier des détails sur les infractions.

Donner suite aux plaintes

La question suivante est le traitement des plaintes. La loi confèrera aux particuliers le droit de se plaindre et de contester la conformité à toute partie de la loi, ce qui leur fera jouer un rôle clé dans les organismes de contrôle. Si la plainte est d'abord adressée à l'entreprise, la tâche de l'autorité de surveillance sera considérablement réduite. Donc, les organisations pourront tirer les leçons de leurs erreurs et faire preuve de leadership sur le marché en les corrigeant et en renforçant la confiance des consommateurs.

Les entreprises devraient jouer un rôle actif dans le contrôle de leurs propres pratiques et elles devraient coopérer avec les consommateurs pour régler les problèmes. Afin de faciliter la vérification de la conformité avec la loi, obligation pourrait être faite aux entreprises de signaler à un organisme de surveillance toute plainte qu'elles reçoivent. Cependant, si un particulier n'est pas satisfait des mécanismes de responsabilité d'une entreprise, il doit exister un autre recours. L'organisme de surveillance devrait être habilité à enquêter et à rechercher un règlement. Il devrait être en mesure soit d'arriver

engagement à respecter la vie privée.

Pour ce faire, on pourrait autoriser une adhésion officielle à la norme de la

CSA par le biais d'un organisme accrédité par le Conseil canadien des normes. Cette solution s'appuierait

sur des mécanismes existants et sur des pratiques volontaires actuelles. Cependant, les entreprises qui

choisiraient de ne pas se soumettre à ces vérifications n'en seraient pas

moins tenues de respecter la loi. Une autre solution consisterait à ne

pas imposer et à ne pas encourager l'inscription ou l'évaluation des

pratiques en matière de gestion de l'information par une tierce partie.

Dans bien des pays dotés de lois visant à protéger les données, la conformité

est supposée, sauf si un litige ou une enquête révèle un problème. Cette

démarche peut comporter une faiblesse, à savoir qu'elle laisse le

soin au public de découvrir les abus, ce qui peut être assez difficile dans

l'environnement actuel de techniques complexes de traitement des données.

Pour remédier à cette faiblesse potentielle, la loi pourrait également

prévoir la vérification de la conformité en habilitant une autorité centrale ou un commissaire à la protection de la

vie privée d'effectuer des recherches, de préparer des rapports sur de nouvelles questions telles que les

nouvelles technologies et de procéder par anticipation à des vérifications ou à des inspections, en plus de répondre à des plaintes. Afin que cela soit aussi

• encourager, sinon obliger, les

organisations à soumettre leurs pratiques en matière de gestion de

l'information à un examen externe afin de démontrer qu'elles sont

conformes à la loi; • s'en remettre uniquement aux

plaintes pour exposer les infractions; • confier à une autorité centrale

dotée de larges pouvoirs le soin de mener des recherches, de

rédigier des rapports et de procéder à des enquêtes.

Les mécanismes d'inscription et de vérification sont valables puisqu'ils

aident à repérer les problèmes au début du processus de mise en œuvre.

Ils permettent également de former le personnel au sein d'une organisation.

Un mécanisme rendant un examen externe obligatoire pourrait, toutefois,

présenter des inconvénients. Il risquerait de placer un lourd fardeau

sur les petites entreprises et sur les organisations qui utilisent peu de

renseignements personnels ou dont les informations sont confidentielles.

Il peut aussi se révéler cher et lourd pour le gouvernement.

Il est peut-être plus viable pour le gouvernement d'encourager les

organisations à faire évaluer leurs pratiques en matière d'information

mais pas de les y obliger. De cette manière, les entreprises pourraient faire preuve de leadership sur le

marché et démontrer un plus grand

Veiller à faire respecter la loi et à faire droit aux plaintes

Une fois les obligations fondamentales et le rôle des codes sectoriels clarifiés, leur respect doit être assuré par le biais d'un régime de surveillance qui permettra de traiter les plaintes et de régler les différends. Ce régime aura pour autre fonction de garantir que le public et les organisations concernées par la loi en connaissent les dispositions et y adhèrent.

La plupart des lois étrangères relatives à la protection des renseignements personnels créent une autorité centrale de surveillance, mais cela varie, notamment dans les États fédéraux. Il serait probablement logique d'utiliser, le cas échéant, les organismes de surveillance existants tels que le Commissariat à la protection de la vie privée du Canada.

Pour concevoir le régime de surveillance le plus pertinent pour le Canada, il faut tenir compte de deux considérations essentielles, soit les pouvoirs nécessaires pour veiller convenablement à l'observation de la nouvelle loi et aux réparations, et la répartition de ces pouvoirs. Il est important de garder à l'esprit que certains types de pouvoirs, comme le pouvoir d'infliger des amendes ou d'ordonner une restitution en cas d'infraktion à la loi, conviennent pour certains organismes de surveillance mais pas pour d'autres. Avec des

Responsabilité

attributions pertinentes, les associations professionnelles, les organes de réglementation et d'autoréglementation existants, un commissariat à la protection de la vie privée et une cour ou un tribunal fédéral pourraient tous jouer un rôle dans la surveillance de la protection de la vie privée. Pour déterminer qui prend les décisions finales, il faut se prémunir contre des conflits d'intérêts possibles.

La première question que doit se poser quiconque sera chargé de surveiller l'application de la nouvelle loi est la suivante : les particuliers et les organisations respectent-ils la loi? La norme de la CSA exige que les entreprises désignent, au sein de l'organisation, un cadre qui sera responsable de la conformité à la loi. Cette obligation deviendrait exécutoire dans la nouvelle loi. On pourrait aussi recourir à des mécanismes supplémentaires pour s'assurer du respect de la nouvelle loi, comme les suivants :

- instituer une obligation d'inscription aux termes de laquelle les organisations font connaître leurs pratiques en matière de gestion de l'information, comme dans le système en place au Royaume-Uni;
- procéder à une vérification initiale afin de s'assurer de l'adhésion à la loi;

Approbation

Une fois les codes sectoriels écrits, qui devrait les approuver et comment?

Manifestement, des codes ayant force exécutoire exigent un processus plus rigoureux que des codes qui apporteraient de simples conseils. Il faut s'efforcer d'éviter de créer une situation de conflit d'intérêts dans laquelle un commissaire à la protection de la vie privée, par exemple, collaborerait à l'élaboration d'un code puis serait chargé de statuer sur les plaintes des consommateurs le concernant.

Que les codes aient force exécutoire ou pas, ils pourraient être approuvés par un organisme public chargé de vérifier s'ils sont conformes à la loi. Par la suite, cet organisme pourrait soumettre les organisations qui appliquent le code à une évaluation afin de déterminer dans quelle mesure elles le respectent et, ensuite, d'approuver le code. Des mesures juridiques ou administratives devraient être prises afin de garantir qu'au cas où le même organisme ait des attributions de supervision, il ne survienne pas de conflit d'intérêts. Il faut comparer ce que coûterait l'approbation des codes par ce type d'organisme, du point de vue du gouvernement et de l'industrie, avec les coûts éventuels associés à d'autres modes d'approbation des codes.

Les codes n'ayant pas force exécutoire pourraient également être vérifiés par :

- un organe accrédité en tant que registraire de la qualité par le Conseil canadien des normes, qui évaluerait les pratiques en matière d'information, comme c'est le cas à présent dans le processus d'inscription à la norme de la CSA; ou
- des vérificateurs internes ou externes ou d'autres parties compétentes en gestion de l'information.

Les codes ayant force exécutoire pourraient également être vérifiés de deux façons :

- par un registraire accrédité. Celui-ci recommanderait de reconnaître la conformité du code avec la loi. Un organisme public ou un fonctionnaire recevrait la recommandation, tiendrait des audiences publiques et donnerait l'approbation finale pour l'approbation.
- par un organisme de surveillance public. Après vérification par cet organisme, un vérificateur autorisé vérifierait les informations afin de s'assurer que le code est appliqué. Après la vérification, les entreprises pourraient demander une exemption ministérielle qui leur permettrait de remplacer les prescriptions de la loi par leurs propres codes sectoriels. Il pourrait être prévu de consulter le public avant d'approuver le code, et le maintien de l'exemption serait assujéti à des vérifications périodiques.

Reconnaissance des codes sectoriels

La nouvelle loi doit-elle reconnaître les codes sectoriels ? Dans

l'affirmative, doivent-ils avoir force obligatoire ou doivent-ils servir uniquement de guides dans l'interprétation des principes de la loi en ce qui concerne des secteurs particuliers ?

D'autres pays ont traité ces questions de diverses façons. La loi québécoise, par exemple, ne fait aucune référence à des codes sectoriels. Néanmoins, plusieurs associations professionnelles dont des membres sont implantés au Québec ont élaboré de tels codes pour leur propre usage.

La loi britannique oblige le registraire de la protection des données à encourager l'élaboration de codes. Ces codes aident à interpréter la Loi, mais ils n'ont pas force de loi. Aux termes de la loi néerlandaise, le Commissaire à la protection de la vie privée est chargé de l'approbation des codes sectoriels. Comme au Royaume-Uni, ces codes n'ont pas force exécutoire, mais ils guident l'interprétation de la Loi. En Nouvelle-Zélande, les codes sectoriels ont pleinement force de loi. Ils peuvent être plus ou moins stricts que les principes énoncés dans la Loi, mais une fois approuvés par le Commissaire à la protection de la vie privée, ils remplacent ces principes. L'élaboration de ces codes est laborieuse, mais il en est résulté le

Code sur la protection des renseignements

médicaux très détaillé et un autre

code pour l'utilisation de numéros d'identité uniques pour la pension

de retraite.

Il existe essentiellement deux façons de reconnaître les codes sectoriels

dans la loi :

- En s'inspirant de ce qui se fait au Pays-Bas, on pourrait encourager les industries à rédiger des codes. Une fois approuvés, ceux-ci guideraient l'interprétation mais n'auraient pas force exécutoire.
- Suivant le modèle néozélandais, les codes approuvés pourraient remplacer les obligations énoncées par la loi et avoir force exécutoire.

Ces options soulèvent une autre question : qui devrait élaborer les codes sectoriels? En demandant aux différents secteurs d'élaborer les codes, on éviterait de placer un fardeau énorme sur des organismes de supervision publics généralement mal placés pour définir eux-mêmes des lignes directrices sectorielles particulières, mais tout a fait capables d'amener les entreprises à nouer un dialogue sur la pertinence du produit fini. Pour élaborer ces codes, les entreprises pourraient puiser dans les compétences croissantes sur la protection des renseignements personnels. Autrement, un organisme public compétent en matière de protection des renseignements personnels pourrait se charger de préparer les codes.

Codes sectoriels en vigueur : Le code modèle de l'Association des banquiers canadiens (ABC) sur la protection des renseignements personnels

L'Association des banquiers canadiens est un leader pour ce qui est de définir des méthodes volontaires visant à protéger les renseignements personnels. En 1986, les banques ont élaboré leur premier code en la matière, qu'elles ont modifié deux fois par la suite. Puis, en 1995-1996, l'ABC a vérifié que son code était conforme à la norme de la CSA.

Price Waterhouse a conclu que le code de l'ABC est conforme au Code de la CSA, et chaque banque s'attache à présent à en appliquer les dispositions par le biais de sons propre code sur la protection des renseignements personnels.

Pour obtenir des exemplaires du code de l'ABC, s'adresser à :
Association des banquiers canadiens
Boîte 348, Commerce Court
Ouest, 30^e étage
Toronto (Ontario) M5L 1G2

Téléphone : (416) 362-6092
Télécopieur : (416) 362-7705

compétences pour interpréter la loi en ce qu'elle vise directement leur activité, et elles voudront peut-être alors rédiger des codes sectoriels qui complèteraient ou remplaceraient les obligations légales.

Les codes sectoriels peuvent être bénéfiques à divers égards. Tout d'abord, ils permettent aux industries de définir leurs propres besoins de renseignements personnels et de démontrer leur attachement au respect de la vie privée en s'autodisciplinant. En démontrant cet attachement et un certain leadership, ils aident à éveiller la confiance des consommateurs et encouragent à protéger ces derniers et à donner l'exemple sur le marché. Ensuite, le processus d'élaboration des codes peut se révéler éducatif et favoriser l'acceptation de bonnes pratiques de gestion de l'information dans l'organisation, et encourager le personnel et la direction à interpréter et à appliquer couramment leurs propres pratiques en la matière. Enfin, l'existence de codes particuliers facilite les vérifications, car ils fournissent un manuel des pratiques relatives à l'information qui peut aider à évaluer les pratiques d'entreprises données.

Codes sectoriels

des renseignements personnels seraient tenues de remplir leurs obligations légales.

Bien des organisations au Canada ont déjà élaboré des codes sur le respect de la vie privée, et certaines les modifient afin de s'aligner sur la norme de la CSA. L'Association des banquiers canadiens, le Bureau d'assurance du Canada et la Fondation des normes de télévision par câble, par exemple, ont déjà publié des codes conformes à la norme. D'autres organisations se sont fixé le même objectif. Les codes sectoriels et les codes des entreprises fournissent des détails et des conseils sur les prescriptions de la loi en ce qui concerne un secteur d'activité ou une entreprise en particulier. D'une certaine manière, ces codes donnent une idée de l'incidence que la loi aura sur les pratiques de traitement de l'information des entreprises qui y sont soumises. Il se peut que nombre d'organisations estiment que les principes de la loi suffisent en eux-mêmes et qu'elles n'ont pas à élaborer leurs propres codes. Ce sera probablement le cas de bien des petites entreprises. Ces organisations devront tout simplement adhérer aux principes énoncés par la loi. D'autres organisations, cependant, préféreront s'appuyer sur leurs propres

Peuvent être en jeu la protection de la santé et de la sécurité d'une ou de plusieurs personnes, des situations d'urgence où il est impossible d'obtenir le consentement de l'intéressé, des recherches médicales, la compilation de statistiques, la conduite d'enquêtes conformes à la loi et le respect des ordonnances judiciaires.

Une deuxième question se pose : les obligations qui ne sont pas énoncées dans la norme de la CSA doivent-elles être prévues par la loi? Par exemple, l'obligation de signaler toute plainte reçue à un organisme public ou celle d'informer le public de ses droits, ou encore de nouvelles obligations imprévues dans la norme originale.

Une troisième vient également à l'esprit : faudrait-il exclure certains renseignements du champ d'application de la loi? Par exemple, la Loi sur la protection des renseignements personnels dans le secteur privé en vigueur au Québec ne s'applique pas aux renseignements recueillis par les journalistes qui sont conservés, utilisés ou communiqués afin d'informer le public.

Théoriquement, il est possible d'intégrer dans la loi les obligations et l'approche de la norme de la CSA en y énonçant les principes fondamentaux, en donnant plus de précisions dans un règlement ou dans un autre instrument tel que des codes sectoriels. Quoi qu'il en soit, les organisations qui utilisent

Si la loi devait reposer sur la norme de la CSA, il faudrait trouver réponse à plusieurs questions.

Pour commencer, la norme de la CSA, qui a été élaborée comme un instrument d'application volontaire, suffit-elle à énoncer les obligations légales ou faudra-t-il y apporter des éclaircissements? Dans toute loi, la précision et la certitude sont importantes, car elles contribuent à faire en sorte que les gouvernements, les consommateurs et les entreprises connaissent clairement leurs droits et obligations respectifs. Cette

clarté est d'autant plus importante lorsqu'un litige entre un particulier et une organisation risque d'avoir des conséquences juridiques. Il sera peut-être nécessaire de préciser d'avantage certaines dispositions de la norme de la CSA, à savoir : quand et comment peut-on recueillir des renseignements personnels et pour quelles raisons, combien de temps une organisation peut conserver ce type de renseignements, quel consentement faut-il obtenir pour leur collecte et sous quelle forme, et quels frais peuvent être facturés pour des copies des dossiers.

La loi devra également préciser dans quelles circonstances exceptionnelles des renseignements personnels peuvent être divulgués à une tierce partie sans le consentement de l'intéressé. Parfois, ces divulgations ne correspondent pas aux fins de la collecte annoncées par l'organisation.

non-respect des principes énoncés ci-dessus en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisme concerné.

La norme de la CSA comprend un commentaire de chacun des dix principes ainsi qu'un guide d'accompagnement qui fournit des conseils plus détaillés sur la mise en application de la norme elle-même. Ces outils aident les entreprises à interpréter la norme et à la mettre en œuvre.

La norme de la CSA présente plusieurs avantages en tant que point de départ pour la loi. Tout d'abord, elle recueille le consensus des principaux intervenants du secteur privé, des organisations de consommateurs et autres groupes d'intérêt public, ainsi que celui d'organismes publics. Ensuite, elle offre une certaine souplesse, car elle a été conçue pour servir de modèle à des codes particuliers à des secteurs d'activité. Enfin, la norme de la CSA est neutre par rapport à la technologie, et ses principes vont au-delà des applications particulières à un secteur. En

conséquence, elle ne sera pas dépassée lorsque les techniques de collecte et de conservation des données changeront. Une loi canadienne idéale s'appuiera sur les succès de l'application volontaire de la norme de la CSA, tout en faisant en sorte que sa mise en œuvre rapide se généralise.

La norme reprend les dix principes suivants en matière de pratiques équitables dans le traitement de l'information :

- **Responsabilité** : Un organisme est responsable des renseignements dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés dans le Code.

- **Détermination des fins de la collecte des renseignements** : Les fins pour lesquelles les renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.
- **Consentement** : Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas indiqué de le faire.

- **Limitation de la collecte** : L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

- **Limitation de l'utilisation, de la communication et de la conservation** : Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis, à moins que la personne concernée n'y consente

- **Exactitude** : Les renseignements personnels doivent être exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés.

- **Mesures de sécurité** : Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

- **Transparence** : Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

- **Accès aux renseignements personnels** : Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettra de les consulter. Il sera possible aussi de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections voulues.

- **Possibilité de porter plainte contre le non-respect des principes** : Toute personne doit être en mesure de se plaindre du

Les rencontres des ministres chargés de l'auotoroute de l'information et des rencontres similaires des ministres chargés de la consommation sont également le cadre d'une collaboration en ce qui concerne la protection des renseignements personnels sur tout le territoire canadien. Elles donnent l'occasion aux ministres de définir des objectifs communs et de s'engager à travailler selon les mêmes critères.

Définir les principes fondamentaux

La première question à se poser dans l'élaboration d'une loi sur la protection des renseignements personnels dans le secteur privé est la suivante : sur quels principes la loi devrait-elle reposer? Puisque l'on retrouve dans toutes les lois du monde le même ensemble élémentaire de pratiques équitables dans le traitement de l'information, on pourrait partir de ces pratiques. Il serait logique, cependant, de s'appuyer sur le consensus réuni autour de notre norme nationale. De nombreuses instances considèrent la norme de la CSA comme une amélioration par rapport aux lignes directrices de l'OCDE. Des principes fondés sur cette norme contribueraient à assurer une compatibilité avec d'autres régimes régs par les lois allant au-delà de ce que préconisent les lignes directrices, comme c'est le cas au Québec.

Au Canada, le secteur privé relève en partie de la compétence fédérale, ce qui est le cas des télécommunications, des banques et du transport interprovincial, et en partie de la compétence provinciale, ce qui est le cas de la santé et de l'éducation. Une protection harmonisée des renseignements personnels couvrant tout le secteur privé serait la meilleure solution, étant donné la mobilité croissante de l'information, et elle éviterait la création de « paradis des données » ou d'obstacles à la libre circulation de l'information. Si l'on veut que tous les Canadiens bénéficient d'une véritable protection globale de leur vie privée, les gouvernements fédéral, provinciaux et territoriaux devront travailler en étroite coopération pour donner lieu à une approche harmonisée dans l'ensemble du pays. Cela est essentiel pour le commerce interprovincial autant que pour le commerce international. La Conférence sur l'harmonisation des lois au Canada (CHLC), groupe indépendant qui préconise l'uniformité des lois dans tout le pays, peut être le cadre d'une telle coopération. Elle a commencé à rédiger en 1995 un avant-projet de loi sur une protection uniforme des données dans le secteur privé, et elle devrait en faire circuler une version pour commentaire en 1998. Une fois terminée, ce modèle pourrait aider les gouvernements fédéral, provinciaux et territoriaux à définir une démarche harmonisée.

Partie 2 : Elaboration de la nouvelle loi canadienne sur la protection des renseignements personnels

La deuxième partie du présent document se penche sur une série de questions qu'il faut régler en préparant la loi afin de protéger les renseignements personnels dans le secteur privé, et propose des solutions à y apporter. Plus particulièrement, la nouvelle loi devra prévoir quatre éléments clés de toute loi sur la protection des données :

- des obligations fondées sur des pratiques équitables de traitement de l'information
- des dispositions administratives pour un organe de surveillance afin de garantir la reddition de comptes des attributions pour des autorités de supervision et des tribunaux
- des pouvoirs et responsabilités qui favoriseront l'information du public et garantiront un réel respect des obligations.

Toute cette section met l'accent sur l'élaboration d'un régime juridique inspiré par les meilleurs aspects des lois étrangères et le succès de la norme de la CSA.

La nouvelle loi canadienne doit :

1. encourager, de la part de ceux qui détiennent des renseignements personnels dans le secteur privé,

des pratiques responsables en ce qui concerne la protection des renseignements personnels;

2. fournir des directives souples mais efficaces pour la protection de droits exécutives et des règles du jeu équitables sur le marché, où les renseignements personnels jouent un rôle de plus en plus important;
3. être flexible, simple, efficace et d'utilisation facile pour les consommateurs, avec des droits exécutives et des mécanismes de recours efficaces;
4. être efficiente, efficace sur le plan administratif, et ne pas imposer un trop lourd fardeau à l'industrie, notamment aux petites entreprises;
5. être conforme à nos obligations internationales.

Garantir une protection nationale

Dans l'élaboration d'un modèle canadien, il faudra se demander comment les gouvernements fédéral, provinciaux et territoriaux se partageront la responsabilité de la protection des renseignements personnels dans le secteur privé.

sont appliquées de manière générale, conférant ainsi aux consommateurs une protection égale. Deuxièmement, en tant qu'instrument d'utilisation volontaire, la norme ne prévoit pas de surveillance ou de possibilité de garantir réparation au consommateur en cas de différend. Une loi souple et efficace fournira le type d'assurance nécessaire pour garantir qu'en cas de problèmes, les consommateurs disposeront de recours.

Quelques-unes des organisations qui se sont prononcées à l'unanimité en faveur du code modèle de la CSA :

- American Express Company
- Association canadienne de la technologie de l'information
- Association canadienne des compagnies d'assurances de personnes inc.
- Association canadienne de télévision par câble
- Association canadienne du marketing direct
- Association des banquiers canadiens
- Bureau d'assurance du Canada
- Cable Television Standards Foundation
- Centre de promotion de l'intérêt public
- Congrès du travail du Canada
- Equifax Canada
- Fédération nationale des associations de consommateurs du Québec
- Information Technology Industry Council
- Sélection du Reader's Digest
- Stentor Telecom Policy Inc.

La norme de la CSA a suscité beaucoup d'intérêt au niveau international. En mai 1996, le groupe de la politique de la consommation de l'Organisation internationale de normalisation (ISO) a adopté à l'unanimité une résolution parrainée par 25 pays approuvant un projet de définition d'une norme internationale de protection des renseignements personnels fondée sur la norme de la CSA. L'ISO étudie à présent la nécessité d'une norme internationale pour protéger la vie privée, mesurer cette protection et assurer une harmonisation mondiale. Si elle accepte la norme de la CSA comme base d'une norme internationale, les entreprises canadiennes qui en appliquent déjà les principes seront sensiblement avantagées.

Le succès remporté par la norme de la CSA place le Canada en bonne position pour passer d'un système de codes d'autoréglementation à une réglementation de la protection des renseignements personnels. La nouvelle loi s'appuiera sur les travaux déjà effectués pour élaborer la norme, ainsi que sur les mesures prises par les diverses industries pour la mettre en œuvre. Moyennant quoi, la loi répondra à deux questions fondamentales. Premièrement, si la norme confère une bonne protection, son application est-elle tout à fait volontaire, de sorte que rien n'en garantisse la mise en œuvre générale. La loi donnera l'assurance que les principes régissant la protection des renseignements personnels

la technologie de l'information, les assurances, la santé et les banques), des groupes de protection des consommateurs, des syndicats et d'autres groupes d'intérêt général afin de discuter de la nécessité d'un code commun pour protéger les renseignements personnels dans le secteur privé.

Cette initiative a débouché sur l'élaboration du *Code type sur la protection des renseignements personnels*, fruit d'un consensus entre tous les intervenants. Le Code, qui repose sur les lignes directrices de l'OCDE, est un ensemble de principes qui s'appliquent à la protection des renseignements personnels dans le secteur privé. Il répond à deux préoccupations générales : la façon dont les organisations collectent, utilisent, divulguent et protègent les renseignements personnels; et le droit de toute personne d'avoir accès à des renseignements la concernant et de pouvoir les faire corriger, si nécessaire. En 1996, le Conseil canadien des normes a déclaré le Code de la CSA norme nationale, faisant du Canada le premier pays au monde à adopter ce type de norme. Tout en démontrant l'attachement continu des parties participantes à des pratiques équitables de traitement de l'information, la norme fournit un instrument qui promet d'être d'utilisation facile pour le consommateur, juste, efficace et efficiente. Elle est le résultat d'une remarquable coopération entre des groupes d'intérêt très différents.

base des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel rédigées en 1980 par l'Organisation de coopération et de développement économiques (OCDE) et signées par le Canada en 1984. Ces lignes directrices visent à protéger les renseignements personnels et à garantir la libre circulation des données.

Elles ont été largement adoptées. On peut voir leur influence dans la loi québécoise destinée à protéger les renseignements personnels dans le secteur privé. Cette influence est visible également dans les lois qui régissent le secteur public au niveau fédéral et dans les provinces suivantes : Colombie-Britannique, Alberta, Saskatchewan, Manitoba, Ontario, Québec et Nouvelle-Écosse, ainsi qu'au Yukon et dans les Territoires du Nord-Ouest. Le Nouveau-Brunswick se prépare à déposer sous peu une loi de ce type.

La norme de la CSA

A l'évidence, il est nécessaire de recentrer le régime actuel de protection de la vie privée dans le secteur privé, mais un travail important a été accompli ces toutes dernières années. Au début des années 1990, l'Association canadienne de normalisation (CSA) a réuni des représentants du secteur public, des secteurs de l'économie (y compris les transports, les télécommunications,

« pratiques équitables de traitement de l'information » qui sont des ensembles de principes relatifs à cette protection. Ces pratiques sont des lignes directrices pour la collecte, l'utilisation, la divulgation, la conservation et l'élimination de renseignements personnels. Ces pratiques varient mais comprennent généralement les principes suivants :

- veiller à ce que le public soit informé des politiques et pratiques relatives à l'information, et à ce que celles-ci soient transparentes
- établir la nécessité et la pertinence des renseignements recueillis
- énoncer une finalité (définir à l'avance les utilisations des données recueillies et les détruire ultérieurement)
- nommer la personne responsable de la protection des renseignements personnels au sein de l'organisation
- obtenir le consentement éclairé de la personne concernée
- assurer l'exactitude et l'exhaustivité des dossiers
- donner l'accès à l'information et le droit d'apporter des corrections

Les pratiques équitables de traitement de l'information sont la pierre angulaire de la plupart des efforts consentis dans le monde pour protéger les renseignements personnels. Elles constituent la

des renseignements personnels. La concurrence peut en devenir déloyale et les règles du jeu, inéquitable. De plus, la confiance des consommateurs dans tout un secteur risque de s'éroder et la confusion peut s'accroître encore en ce qui concerne les droits et les règlements.

Assurer la protection efficace des renseignements personnels peut s'avérer essentiel pour que le Canada reste concurrentiel à l'échelle internationale dans l'économie de l'information mondiale. Cela peut, par exemple, influencer sur l'échange de données avec les pays membres de l'Union européenne. En 1995, l'Union européenne a adopté la *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. Cette directive vise à harmoniser les pratiques en matière de protection des données au sein de l'Union européenne et impose, notamment, aux États membres d'adopter des lois pour protéger les renseignements personnels dans les secteurs public et privé. Ces lois doivent empêcher le transfert d'information vers des États non-membres qui ne garantissent pas un degré de protection « adéquat ».

Cette directive peut faire de la protection des renseignements personnels un obstacle non tarifaire majeur au commerce avec le Canada. En effet, s'il ne peut assurer une protection suffisante des

renseignements personnels, le Canada risque de voir la « circulation des données » avec l'Union européenne bloquée. Sans loi détaillée de la protection des données, les entreprises canadiennes devront peut-être négocier individuellement des contrats afin de respecter les règles de l'Union européenne. En plus de l'incertitude qui risque de l'entourer, ce processus pourrait prendre du temps et devenir coûteux. La protection des informations venant de l'étranger pourraient aussi être soumise à des normes supérieures à celles qui s'appliquent aux données canadiennes. Ces pressions, entre autres, s'accroîtront probablement dans les années à venir. À cause du défi que pose la concurrence dans le commerce électronique, nous n'avons pas le temps de renforcer progressivement la protection des renseignements personnels et la confiance des consommateurs. En outre, les citoyens ont raison de demander une protection pertinente dans la nouvelle économie numérique. Il est donc important d'agir maintenant afin d'élaborer une loi qui prévoira les défis actuels et futurs, et y répondra comme il convient.

Protection des renseignements personnels : les règles du jeu

La plupart du temps, la réglementation de la protection des renseignements personnels commence par la définition de

pressions sur les lois et les règlements existants. Par exemple, l'accès à Internet figure maintenant dans les gammes de produits qu'offrent les compagnies de téléphone et de cablodistribution, de même que de nombreuses petites entreprises. Or, comme ces secteurs sont soumis à des réglementations différentes ou ne sont pas réglementés, ce type de convergence risque de semer la confusion dans l'esprit des consommateurs, qui ne sauront pas quelles règles s'appliquent à quelles entreprises et dans quelles circonstances, et qui ne sauront pas non plus à qui se plaindre en cas de problème.

Certaines organisations ont bien réagi au delà de la protection des renseignements personnels et elles ont adopté des codes d'autoréglementation qui régissent la collecte et l'utilisation de renseignements personnels. Ainsi, l'Association canadienne du marketing direct demande à ses membres d'obéir à un code d'éthique qui comporte des règles en matière de collecte et d'utilisation des renseignements personnels. Cependant, tous ceux qui font du marketing direct n'appartiennent pas à l'association, et rien ne les oblige à suivre les mêmes règles. Toutes les entreprises et toutes les associations professionnelles n'ont pas pris de mesures volontaires, et certaines entreprises sont peut-être tentées à court terme d'ignorer de telles mesures et de faire un mauvais usage

les anciens systèmes de dossiers sur papier, l'information était forcément divisée, dans les nouveaux systèmes, il est facile et peu coûteux de combiner les données tirées de nombreuses sources pour créer un profil ou prendre des décisions.

Par ailleurs, la législation visant l'information détenue par le secteur public ne tient pas compte du fait qu'aujourd'hui, le secteur privé recueille et utilise beaucoup de renseignements personnels. On s'est toujours inquiété de ce que les gouvernements détiennent quant à de données sur les citoyens, ce qui a entraîné des mesures législatives visant à limiter l'utilisation de ces données et à autoriser les citoyens à voir les dossiers les concernant et à demander que des corrections y soient apportées, le cas échéant. Cependant, à mesure que nous avançons dans l'économie et la société de l'information, et que l'information elle-même devient une marchandise, le secteur privé recueille et utilise de plus en plus de renseignements personnels sur le marché et dans la prestation de services publics par des tiers. Il est important de tenir compte de cette tendance dans une nouvelle loi qui garantisse l'application de lignes directrices communes dans la manipulation et le traitement de ces renseignements.

Qui plus est, la convergence de différents secteurs de l'économie auparavant distincts crée de nouvelles

d'éléments qui contribuent au rôle de plus en plus important de l'information dans l'économie mondiale. Dans cette nouvelle économie mondiale, l'information est un bien précieux qui peut être porteur d'emplois, de prospérité et d'un meilleur service à la clientèle. Si l'on y ajoute d'autres facteurs clés, il devient de plus en plus pressant de recueillir et d'utiliser comme jamais auparavant des renseignements personnels.

Puisque plus de la moitié des Canadiens sont d'avis que l'inforoute réduit la vie privée au Canada¹, il est essentiel à la croissance de l'économie de l'information canadienne que les consommateurs aient confiance dans le système. Une loi qui définit un ensemble de règles communes pour la protection des renseignements personnels aidera à renforcer cette confiance et à instaurer un système équitable où l'usage abusif de renseignements personnels ne pourra conférer un avantage concurrentiel. D'autre part, les progrès réalisés en matière d'outils de navigation et l'apparition de logiciels complexes font que les renseignements ne sont plus conservés uniquement dans des bases de données centrales, mais peuvent être diffusés sur tous les réseaux d'une organisation. C'est en grande partie à cause de cela que la protection actuelle ne suffit plus. Les frontières géographiques n'ont plus la même importance. Et si, dans

de renseignements personnels. La Commission d'accès à l'information, qui veille à son application, est chargée des enquêtes et du règlement des différends.

Dans le reste du Canada, la protection est sporadique et inégale dans le secteur privé. Nombre de secteurs ne sont soumis à aucune règle en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements personnels, mais quelques-uns sont couverts par ce que le Commissariat à la protection de la vie privée du Canada décrit comme un « ensemble de lois, de règlements et de codes. Cet ensemble se compose de diverses lois fédérales et provinciales, d'où une protection incomplète, voire incohérente. Même s'il donne des résultats dans certains secteurs, il n'établit pas de principes communs pour tous et tous ne sont pas visés. Ce côté incomplet de la législation explique l'incertitude des entreprises et l'absence de protection uniforme des consommateurs. Et si l'ensemble de lois disparates a une utilité relative, il n'en est pas moins inadéquat face à l'évolution du monde.

Pourquoi la protection actuelle ne suffit plus

De nouvelles technologies, la collecte croissante de données dans le secteur privé, l'évolution des tendances du marché et le nouveau marché mondial qui s'ouvre au commerce électronique, voilà autant

1. Ekos Research Associates Inc., "Information Highway and the Canadian Communication Household, Draft Wave 1 Report," janvier 1998.

Partie 1 : Qu'entend-on par protection des renseignements personnels?

Quelle protection existe-t-il aujourd'hui?

Le gouvernement fédéral et la plupart des provinces ont des lois qui régissent la collecte, l'utilisation et la divulgation de renseignements personnels par le secteur public. La loi fédérale sur la protection des renseignements personnels (1985) s'applique à tous les ministères fédéraux, à la plupart des organismes fédéraux et à certaines sociétés d'État canadiennes. Le Commissariat à la protection de la vie privée du Canada, qui veille à l'application de la Loi, est habilité, en autres, à recevoir des plaintes, à mener des enquêtes et à essayer de régler les différends. Il peut aussi formuler des recommandations. Les différends relatifs au droit d'accès à des renseignements personnels qui ne sont pas résolus de cette manière peuvent être portés devant la Cour fédérale du Canada pour être soumis à un examen judiciaire.

Le secteur privé fonctionne différemment. À ce jour, seul le Québec a adopté une loi d'ensemble sur la protection des renseignements personnels visant le secteur privé. La Loi sur la protection des renseignements personnels dans le secteur privé fournit un cadre détaillé en ce qui concerne la collecte, l'utilisation et la divulgation

Lors de sondages successifs, les Canadiens se sont déclarés préoccupés par le respect de leur vie privée en général et par la perte de contrôle sur des renseignements à caractère personnel, en particulier. On parle alors de protection des renseignements, c'est-à-dire du droit de chacun à décider quand, comment et dans quelle mesure il souhaite partager avec autrui des renseignements personnels.

La protection des renseignements est importante pour plusieurs raisons. Tout d'abord, elle est liée à un ensemble d'autres droits et valeurs tels que la liberté, la liberté d'expression et la liberté d'association. Si l'on ne peut exercer de contrôle sur les renseignements à caractère personnel, nous risquons de voir ces droits brimés. Ensuite, plus les renseignements nous concernant sont connus, plus ils sont utilisés dans diverses situations pour prendre des décisions à propos, par exemple, des types de services auxquels nous avons droit, des emplois pour lesquels nous sommes qualifiés et des avantages dont nous pouvons bénéficier. Il est très important qu'il existe des mécanismes qui nous permettent de protéger des renseignements personnels et de nous assurer qu'ils sont exacts et pertinents.

seront utilisés et d'avoir l'assurance qu'ils seront protégés. Parallèlement, une telle loi apportera à nos partenaires commerciaux du monde entier l'assurance dont ils ont besoin pour entreprendre des transactions qui nécessitent le transfert international de renseignements personnels. Le présent document de travail vise à obtenir votre avis sur ce que constitue un juste équilibre dans la nouvelle loi. Il énonce les principaux points à traiter, expose, dans les grandes lignes, certaines options quant à la loi, puis soumet quelques questions précises à votre réflexion. Votre avis est important, car il nous aidera à faire en sorte que la nouvelle loi tienne compte de divers intérêts tout en renforçant la confiance des Canadiens dans les transactions électroniques.

pour protéger les renseignements personnels dans le secteur privé. En septembre 1996, le ministre de la Justice a réitéré cet engagement et précisé que le gouvernement entendait légiférer d'ici l'an 2000. Les ministres de l'Industrie et de la Justice ont été chargés d'élaborer ensemble la loi, après consultation des provinces, des territoires et d'autres intervenants. Si l'on veut faire du Canada un leader mondial en matière de commerce électronique, il est important, pour renforcer la confiance des consommateurs et la stabilité du marché, d'adopter une loi qui trouve le juste équilibre entre le besoin des entreprises de recueillir, conserver et utiliser des renseignements personnels et le besoin des consommateurs de savoir comment ces renseignements

Pour que le commerce électronique se développe au Canada, il faut un milieu stable, prévisible et favorable dans lequel particuliers, institutions et entreprises soient à l'aise, confiants et en sécurité. Il faut également, à l'échelle internationale, des règles permettant aux particuliers, aux institutions et aux entreprises d'échanger facilement des renseignements, des produits et des services d'un pays à l'autre, dans le monde entier, en toute sécurité et avec des résultats prévisibles. Le présent document fait partie d'une série de documents sur le commerce électronique dont l'objectif est de connaître votre avis sur l'établissement de règles stables et prévisibles destinées à favoriser l'essor du commerce électronique au Canada et l'édification d'une économie et d'une société de l'information au Canada.

Protéger les renseignements personnels

Le défi de l'ère électronique est qu'à chacune de nos transactions, nous laissons des données retraçables qui, combinées, peuvent révéler des détails personnels et nos préférences.

À cause de la numérisation des dossiers médicaux, des dossiers scolaires, des dossiers d'emploi et de consommation, il devient possible, en combinant des renseignements, de tracer le profil d'un consommateur, et ce, à partir de données que la plupart d'entre nous estiment très personnelles. Ces renseignements peuvent être transmis d'une province à l'autre, voire d'un pays à l'autre, être vendus, réutilisés ou intégrés dans d'autres bases de données sans que nous le sachions ou y consentions.

En tant que consommateurs et citoyens, lorsque nous magasinons ou que nous planifions des vacances sur Internet, lorsque nous effectuons des transactions bancaires à domicile, cherchons un emploi, communiquons avec des amis ou des parents, lorsque nous faisons des achats avec des cartes de débit, trouvons des renseignements médicaux, ou lorsque nous concluons d'autres sortes de transactions électroniques, nous devons avoir l'assurance que nous avons pris sur les renseignements qui nous concernent et que ceux-ci bénéficient d'une protection élémentaire.

Le gouvernement du Canada s'est engagé à définir des règles claires et prévisibles qui régiront la protection des renseignements personnels. En mai 1996, suite à une recommandation du Comité consultatif sur l'autoroute de l'information, le ministre de l'Industrie a annoncé que le gouvernement fédéral élaborerait une loi

Introduction : Pour une économie et une société de l'information au Canada

Un Canada branché

« Nous mettrons l'infrastructure de l'information et du savoir à la portée de tous les Canadiens d'ici l'an 2000, ce qui fera du Canada le pays le plus « branché » du monde . . . Un pays branché, c'est beaucoup plus qu'un réseau de fils, de câbles, et d'ordinateurs. C'est un pays où les citoyens ont accès aux compétences et aux connaissances dont ils ont besoin pour profiter de l'infrastructure du savoir et de l'information qui évolue si rapidement. C'est aussi un pays dont les citoyens sont reliés les uns aux autres. »

Discours du Trône,
23 septembre 1997.

Là réussite du Canada au ^{XXI}e siècle sera largement fondée sur la capacité des Canadiens et des Canadiennes de participer pleinement à l'économie mondiale du savoir et d'y réussir. Or, pour garantir cette réussite, nous devons tous — particuliers, secteur privé et tous les paliers de gouvernement — bâtir rapidement au Canada une économie et une société de l'information. Pour sa part, le gouvernement du Canada s'est engagé à donner aux Canadiens et aux Canadiennes accès à l'information et à des connaissances qui leur permettront, à eux-mêmes et à leurs collectivités, à leurs entreprises et à leurs institutions, de trouver de

nouvelles possibilités d'apprendre, de nouer de liens, de faire des transactions, et de développer leur potentiel économique et social. Tel est l'objectif du raccordement des Canadiens à l'infonroute — découvrir tout un univers de possibilités économiques et sociales en tirant parti des nouvelles technologies, de l'infrastructure de l'information et du contenu multimédia pour favoriser le développement et la croissance des entreprises; créer des emplois novateurs; améliorer les communications directes avec nos concitoyens et avec nos institutions et nos services publics; et relier le Canada au monde entier.

Le commerce électronique, qui est au coeur de l'économie de l'information, se définit comme un ensemble de transactions et d'activités commerciales informatiques et électroniques, comprenant, en règle générale, le traitement et la transmission de données et de renseignements numérisés. Ainsi, le commerce électronique peut comprendre l'échange de sommes importantes entre des institutions financières, l'échange de données informatiques entre grossistes et détaillants, des transactions bancaires par téléphone, et l'achat de biens et de services sur Internet.

Table des matières

Introduction : Pour une économie et une société	1
de l'information au Canada	1
Un Canada branché	1
Protéger les renseignements personnels	2
Partie 1 : Qu'entend-on par protection des renseignements personnels?	5
Quelle protection existe-t-il aujourd'hui?	5
Pourquoi la protection actuelle ne suffit plus	6
Protection des renseignements personnels : les règles du jeu	8
La norme de la CSA	9
Partie 2 : Elaboration de la nouvelle loi canadienne sur la	
protection des renseignements personnels	13
Garantir une protection nationale	13
Définir les principes fondamentaux	14
Codes sectoriels	17
Reconnaissance des codes sectoriels	19
Approbation	20
Veiller à faire respecter la loi et à faire droit aux plaintes	21
Responsabilité	21
Donner suite aux plaintes	23
Organismes de surveillance	24
Education du public	25
Arriver à un juste équilibre dans la loi canadienne	26
Partie 3 : La parole est à vous	27
Obligations	27
Pouvoirs	27
Répartition des attributions	28
Coopération	28
Annexe : Documents de référence	29
Glossaire	30

La protection des renseignements personnels — Pour une économie et une société de
Web d'Industrie Canada (<http://strategis.ic.gc.ca/vieprivee>) et sur le site Web de Justice
Canada (<http://canada.justice.gc.ca>).

Le présent document peut être fourni dans d'autres versions aux personnes handicapées
qui en font la demande.

Pour obtenir des exemplaires du présent document de travail, veuillez vous adresser aux :

Services de distribution

Direction générale des communications

Industrie Canada

Bureau 205D, tour Ouest

235, rue Queen

Ottawa (Ontario) K1A 0H5

Téléphone : (613) 947-7466

Télecopieur : (613) 954-6436

Si vous souhaitez avoir des précisions sur le contenu du présent document de travail et sur
le processus de consultation, ou soumettre vos commentaires sur le document, veuillez
communiquer avec :

Helén McDonald

Directrice générale, Développement des politiques

Groupe de travail sur le commerce électronique

Industrie Canada

300, rue Slater, 20^e étage

Ottawa (Ontario) K1A 0C8

Télecopieur : (613) 957-8837

Courriel électronique : vieprivee@ic.gc.ca

Renseignements par téléphone : (613) 990-4255

Vous avez jusqu'au 27 mars 1998 pour nous faire parvenir vos commentaires en faisant
référence à l'avis n° IPPB-002-98 publié dans la Partie I de la *Gazette du Canada* le
24 janvier 1998 et intitulé *Publication d'un document de discussion sur la protection des*
renseignements personnels sur le marché ainsi qu'au titre du présent document.

Deux semaines après cette date limite et durant une période d'un an, le public pourra
consulter tous les commentaires aux heures normales d'ouverture des bureaux, à
l'adresse suivante :

Bibliothèque d'Industrie Canada

3^e étage, tour Ouest

235, rue Queen

Ottawa (Ontario) K1A 0H5

et dans les bureaux régionaux d'Industrie Canada à Halifax, Montréal, Toronto, Edmonton
et Vancouver.

© Sa Majesté la Reine du chef du Canada
(Industrie Canada/Justice Canada) 1998

N° de catalogue C2-336/1998

ISBN 0-662-633-26-1

51730B



La protection des renseignements personnels

Pour une économie et une
société de l'information
au Canada

Groupe de travail sur le commerce électronique
Industrie Canada
Justice Canada
janvier 1998

La protection des renseignements personnels

Pour une économie et une
société de l'information
au Canada

